TABLA DE EQUIVALENCIA FUNCIONAL ENTRE ESTÁNDARES DE SEGURIDAD Y LA LFPDPPP, SU REGLAMENTO Y LAS RECOMENDACIONES EN MATERIA DE SEGURIDAD DE DATOS PERSONALES

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

ÍNDICE

1. INTRODUCCIÓN A LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES EN MÉXICO

1.1 Constitución Política de los Estados Unidos Mexicanos

Con la reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que tuvo lugar en el año 2009, se incorporó a la lista de los derechos humanos y sus garantías, el derecho a la protección de datos personales, y se le dotó de contenido, al señalar nuestra Carta Magna que:

> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

En ese sentido, en nuestro país, la protección de datos personales se considera un derecho humano.

1.2 Ley Federal de Protección de Datos Personales en Posesión de los Particulares

El 6 de julio de 2010 entró en vigor la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP o la Ley), la cual tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, y con ello garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. La Ley aplica a los particulares que traten datos personales, sean personas físicas o morales, a quienes la Ley denomina responsables. Es importante señalar que la Ley define al

tratamiento como "la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales".

El derecho a la protección de los datos personales en posesión de los particulares se encuentra regulado en México con base en ocho principios: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Los responsables están obligados a tratar los datos personales atendiendo las obligaciones que se imponen a través de estos ocho principios.

El principio de licitud obliga a los responsables a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional. Por su parte, el principio de consentimiento establece que los responsables deberán obtener el consentimiento de los titulares para el tratamiento de los datos personales, a menos que no sea exigible de acuerdo con las excepciones que prevé el artículo 10 de la Ley. El consentimiento puede ser tácito, expreso o expreso y por escrito, según el tipo de datos personales que se traten, pero en todo caso debe ser libre, específico e informado. Con relación a esto último, el principio de información señala como obligación de los responsables poner a disposición de los titulares el aviso de privacidad, previo a la obtención de los datos personales, a fin de informarles sobre las características principales del tratamiento y la forma en que podrán ejercer sus derechos.

Asimismo, el principio de calidad se cumple cuando los datos personales tratados por los responsables son exactos, completos, correctos y actualizados. El principio de finalidad señala que los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades determinadas o concretas establecidas en el aviso de privacidad. Ligado a lo anterior, el principio de proporcionalidad establece que sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.

Por último, el principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad; mientras que el principio de responsabilidad señala que el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado. Para cumplir con el principio de responsabilidad, el responsable podrá valerse de estándares, mejores prácticas, políticas internas, esquemas de autorregulación o cualquier otro mecanismo que considere adecuado para tales fines.

Ahora bien, además de los ocho principios antes descritos, la Ley prevé dos deberes: el de seguridad de los datos personales y el de confidencialidad. Este último refiere a la obligación de los responsables y encargados que intervengan en cualquier fase del tratamiento de datos personales, de guardar confidencialidad respecto de la información personales que esté en su posesión, aún después de que finalice la relación con el titular.

Y con relación al deber de seguridad de los datos personales, la Ley establece en su artículo 19 que "Todo responsable que lleve a cabo el tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado". De manera adicional, en el artículo 20, la Ley señala que "las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de manera significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos".

Asimismo, la Ley establece otra serie de obligaciones que deberán cumplir los responsables del tratamiento de datos personales, entre las que destaca la de atender

las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) que presenten los titulares.

Por otra parte, la Ley nombra al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto), actualmente reconocido como órgano constitucional autónomo, como la autoridad garante del derecho a la protección de datos personales en posesión de los particulares, y para ello le otorga facultades informativas, normativas, en materia de verificación, resolutorias, preventivas, en materia de cooperación nacional e internacional y sancionadoras.

En el caso que nos ocupa, nos interesa destacar las facultades del INAI para divulgar estándares y mejores prácticas en materia de seguridad de la información, en la cual se basa la presente Tabla de Equivalencia.

En uso de las facultades que le otorga la Ley, el Instituto sustancia tres tipos de procedimientos: el de protección de derechos, enfocado a los derechos ARCO; el de verificación, a fin de vigilar en debido cumplimiento de la norma, y el de imposición de sanciones.

Con relación a este último procedimiento, la Ley faculta al INAI a establecer sanciones que van desde 100 a 320 mil días de salario mínimo vigente en el Distrito Federal, a los responsables que comentan las infracciones que prevé la propia Ley en su artículo 63. En caso de reincidir, se impondrá un castigo adicional similar al anterior, además de que podrán incrementarse hasta por dos veces los montos establecidos cuando se trate de datos sensibles.

Asimismo, se impondrán penas corpóreas de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo custodia. Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos

personales mediante el engaño, aprovechándose del error en que se encuentre el titular o persona autorizada para transmitirlos.

1.3 Reglamento de la LFPDPPP

En particular, con relación al deber de seguridad de los datos personales, que es la materia principal de esta Tabla de Equivalencia, el Reglamento de la Ley, en su Capítulo III, detalla los factores y acciones que deberán tomar en cuenta tanto responsables, como encargados, para la seguridad de los datos personales.

Al respecto, el artículo 60 del Reglamento de la Ley señala:

> *Artículo 60. El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:*
>
> *I. El riesgo inherente por tipo de dato personal;*
> *II. La sensibilidad de los datos personales tratados;*
> *III. El desarrollo tecnológico, y*
> *IV. Las posibles consecuencias de una vulneración para los titulares.*
>
> *De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:*
> *I. El número de titulares;*
> *II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;*
> *III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y*
> *IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.*

Por su parte, el artículo 61 del Reglamento establece:

Artículo 61. A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:

I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
II. Determinar las funciones y obligaciones de las personas que traten datos personales;
III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
VII. Llevar a cabo revisiones o auditorías;
VIII. Capacitar al personal que efectúe el tratamiento, y
IX. Realizar un registro de los medios de almacenamiento de los datos personales.

El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.

Asimismo, el artículo 62 del Reglamento dice:

Artículo 62. Los responsables deberán actualizar la relación de las medidas de seguridad, cuando ocurran los siguientes eventos:

I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable;
II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo;
III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 del presente Reglamento, o
IV. Exista una afectación a los datos personales distinta a las anteriores.

En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.

En cuanto a las vulneraciones de seguridad, los artículos 63, 64, 65 y 66 señalan:

Vulneraciones de seguridad
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

Notificación de vulneraciones de seguridad
Artículo 64. El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Información mínima al titular en caso de vulneraciones de seguridad
Artículo 65. El responsable deberá informar al titular al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener más información al respecto.

Medidas correctivas en caso de vulneraciones de seguridad

> *Artículo 66. En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.*

No se omite señalar que, por su parte, el artículo 58 del Reglamento de la Ley señala que en los casos en que ocurra una vulneración a la seguridad de los datos personales, el Instituto podrá tomar en consideración el cumplimiento de sus recomendaciones para determinar la atenuación de la sanción que corresponda.

1.4 Recomendaciones en materia de seguridad de datos personales

En las Recomendaciones en materia de Seguridad de Datos Personales, publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013, el INAI recomienda la implementación de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), para la protección de los datos personales.

Estas recomendaciones se basan en la seguridad a través de la gestión del riesgo de los datos personales, entendiéndose de forma general al riesgo como una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que al determinar el riesgo en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Es importante señalar que la adopción de las recomendaciones es de carácter voluntario, por lo que los responsables y encargados podrán decidir libremente qué metodología conviene más aplicar en su negocio para la seguridad de los datos personales. Asimismo, el seguimiento de las presentes recomendaciones no exime a los responsables y encargados de su responsabilidad con relación a cualquier vulneración que pudiera ocurrir a sus bases de datos, ya que la seguridad de dichas bases depende de una correcta implementación de las medidas de seguridad.

2. IMPORTANCIA DE LA TABLA DE EQUIVALENCIA

2.1 Definición

La Tabla de Equivalencia es un material de referencia para los responsables y encargados, que les permitirá evaluar si la implementación de determinados estándares internacionales en materia de seguridad de la información y privacidad en su organización facilitan el cumplimiento de los requisitos y obligaciones que establece la Ley y su Reglamento en lo relativo a medidas de seguridad, así como las Recomendaciones en materia de Seguridad de Datos Personales emitidas por el Instituto y publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013.

2.2 Beneficios

Las ventajas de la Tabla de Equivalencia son las siguientes:

1) Proporciona apoyo técnico a los responsables y encargados en la protección de datos personales.
2) Se basa en estándares internacionales relacionados con la seguridad de la información y privacidad, de amplia aceptación en las organizaciones mexicanas.
3) Ayuda a determinar si la implementación de los controles que se establecen en los estándares internacionales relacionados con la seguridad de la información y privacidad facilitan el cumplimiento de las obligaciones y requisitos establecidos por la LFPDPPP y su Reglamento, y si se adaptan a las Recomendaciones en materia de seguridad de datos personales.
4) Facilita a los responsables y encargados el cumplimiento de sus obligaciones en materia de seguridad de los datos personales.
5) Ayuda a disminuir el impacto en cuanto a costos de implementación de la LFPDPPP y su Reglamento.

6) Enriquece el objeto de los esquemas de autorregulación vinculante en materia de protección de datos personales.
7) Ayuda a que los responsables y encargados demuestren ante el Instituto el cumplimiento de las obligaciones previstas en la LFPDPPP y su Reglamento, y a lo previsto en las Recomendaciones en materia de seguridad de datos personales.

3. NIVEL DE CONTRIBUCIÓN

A continuación se muestra el nivel de contribución de los estándares internacionales en materia de seguridad de la información y privacidad que son objeto de este análisis, para lograr el cumplimiento de los requisitos contenidos en la Ley, su Reglamento, y las Recomendaciones en materia de seguridad de datos personales.

Para el cálculo del nivel de contribución, se tomó como base el total de requisitos de la Ley, su Reglamento, y las Recomendaciones, que componen la Tabla de Equivalencia. **Así, un estándar tiene un nivel de contribución Alto cuando cumple el 87% o más de los requisitos exigidos por la norma; un nivel de contribución Medio cuando cumple del 60% al 87% de los requisitos, y un nivel de contribución Bajo cuando cumple con menos del 60% de los requisitos.**

Simbología del Nivel de Contribución

La siguiente tabla muestra el resumen del análisis, según el nivel de contribución por estándar:

Estándar	Nivel de Contribución
ISO/IEC 27001 (2005, 2013), Information Technology - Security techniques – Information security management systems – Requirements.	
ISO/IEC 27002 (2005, 2013), Information Technology - Security techniques – Code of practice for security management.	

Estándar	Nivel de Contribución
ISO/IEC 27005:2008, Information Technology - Security techniques – Information security risk management.	
ISO/IEC 27006:2011, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.	
ISO/IEC TR 27008:2011, Information technology -- Security techniques -- Guidelines for auditors on information security controls.	
ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.	
ISO/IEC 20000-1:2011 Information technology - Service management -Part 1: Service management system requirements.	
ISO 22301:2012 Societal security - Business continuity management systems – Requirements.	
ISO 31000:2009, Risk management – Principles and guidelines.	
ISO GUIDE 72, Guidelines for the justification and development of management systems standards.	
ISO GUIDE 73, Risk management – Vocabulary.	
ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary.	

Estándar	Nivel de Contribución
BS 10012:2009 Data protection – Specification for a personal information management system.	
NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.	
OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.	
Generally Accepted Privacy Principles (GAPP) from American Institute of CPAs.	
Control Objectives for Information and Related Technology (COBIT 4.1).	
Control Objectives for Information and Related Technology (COBIT 5).	
PCI DSS, Payment Card Industry Data Security Standard.	
HIPAA, Health Insurance Portability and Accountability Act.	
SOx, Sarbanes-Oxley Act of 2002.	
ITIL, Information Technology Infrastructure Library.	
The Open Web Application Security Project (OWASP).	
Cloud Security Alliance Cloud Controls Matrix (CCM).	

4. ANÁLISIS POR ESTÁNDAR

A continuación se muestran los objetivos de control de cada estándar internacional en materia de seguridad de la información y privacidad, que tienen una contribución para lograr el cumplimiento de las obligaciones contenidas en la Ley, su Reglamento, y las Recomendaciones en materia de seguridad de datos personales.

4.1 ISO/IEC 27001:2013, Information Technology - Security techniques – Information security management systems – Requirements.

Introducción. El estándar proporciona los requerimientos para establecer, controlar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (ISMS: Information Security Management System). La adopción de este sistema de gestión es una decisión estratégica de las organizaciones, la cual se debe basar en los riesgos y objetivos de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	RESPONSABLE					
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.
					6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado al cumplimiento de los objetivos de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
					8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
					9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
	LICITUD Y LEALTAD					
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
	CONSENTIMIENTO					

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
	INFORMACIÓN					
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
	CALIDAD					
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	4 Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
	FINALIDAD					
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.				planeación para alcanzarlos.	objetivos.
	PROPORCIONALIDAD					
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
	CONFIDENCIALIDAD					
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
	RESPONSABILIDAD					
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					5. Liderazgo.	Definición del compromiso y las responsabilidades de la Dirección en un ISMS. Asignación de los roles relevantes para el ISMS.
					6. Planeación.	Direccionamiento de riesgos y oportunidades en lo que a seguridad se refiere orientado

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						al cumplimiento de los objetivos de la organización.
					7. Soporte.	Aprovisionamiento apropiado de los recursos técnicos, humanos y financieros para el establecimiento del ISMS.
					8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS.
					9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.2 Competencia.	El personal al que sean asignados roles dentro del ISMS debe contar con las aptitudes apropiadas de acuerdo al nivel de responsabilidad.
					7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	7.1 Recursos.	Asignación de los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora del ISMS.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
					5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis	6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratamiento.			de Brecha.	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
					5.3 Roles, responsabilidades, y autoridades organizacionales.	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a seguridad de la información sean correctamente asignados y comunicados.
	SEGURIDAD					
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Información.	aceptada por la dirección.
	No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.1 Liderazgo y compromiso.	La dirección debe demostrar compromiso dentro del establecimiento, implementación, mantenimiento y mejora al ISMS.
					5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					5.3 Roles, responsabilidades, y autoridades	La dirección realiza actividades para asegurar que los roles y responsabilidades en cuanto a

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					organizacionales.	seguridad de la información sean correctamente asignados y comunicados.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo	6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				para la Implementación de las Medidas de Seguridad Faltantes.		alinear los planes al logro de los objetivos del ISMS.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.2 Competencia.	El personal al que sean asignados roles dentro del ISMS debe contar con las aptitudes apropiadas de acuerdo al nivel de responsabilidad.
					7.3 Concientización.	Actividades para dar a conocer en la organización el ISMS, la política de seguridad y crear compromiso de los empleados.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	7.5 Información documentada.	Toda la información relacionada al ISMS debe ser documentada.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	8. Operación.	Proceso para definir las actividades para: planear, implementar, monitorear y mejorar el ISMS
					9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos.
					10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
	VULNERACIONES A LA SEGURIDAD					

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	7.4 Comunicación.	Determinar las actividades de comunicación necesarias a las partes relevantes ya sean internos o externos a la organización.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas,		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la	9. Evaluación del desempeño.	Actividades para evaluar el desempeño y la efectividad del ISMS respecto a las métricas y objetivos definidos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.			Información.	10. Mejora.	Proceso a seguir para mejorar lo adecuado del ISMS respecto a los objetivos planeados.
	ENCARGADO					
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación,		Art. 50	1. Recomendación General.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.
					6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	o cuando así lo requiera la autoridad competente.					
	SUBCONTRATACIONES					
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.					
	CÓMPUTO EN LA NUBE					
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
					6.1.2 / 8.2 Evaluación de riesgos de Seguridad de la Información.	Se realizan evaluaciones de riesgo en intervalos planeados con base en una metodología aceptada por la dirección.
					6.1.3 / 8.3 Tratamiento de riesgos de Seguridad de la Información.	Definición de un plan de tratamiento de riesgos de acuerdo a la evaluación realizada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
					8.1 Planeación y Control Operacional.	Actividades para conocer los requerimientos en cuanto a seguridad de la información y alinear los planes al logro de los objetivos del ISMS.
	TRANSFERENCIAS					
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	4. Contexto de la Organización.	Identificación de factores internos y externos relevantes para la organización, partes involucradas y alcance del ISMS.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	5.2 Política.	La dirección debe establecer una política de seguridad de la información acorde a los objetivos de la organización.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.2 Objetivos de Seguridad de la Información y planeación para alcanzarlos.	Definición de los objetivos del ISMS y asignación de los recursos para cubrir dichos objetivos.

4.2 ISO/IEC 27002:2013, Information Technology - Security techniques – Code of practice for security management.

Introducción. . El ISO 27002:2013 es el código de prácticas de seguridad de la información el cual tiene como objetivo proveer una guía para la implementación de controles para el Sistema de Gestión de Seguridad de la Información ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
					6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
					7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
					8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
					10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
					11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
					12 Seguridad en las operaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
					13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
					14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
					15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
					16 Gestión de Incidentes de Seguridad de la	Actividades para la gestión de incidentes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Información.	
					17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.
					18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	que persigue el sujeto regulado.				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.					
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.					utilizados.
					11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
					11.2.7 Eliminación segura o re-uso del equipo.	Actividades para el re-uso o la eliminación de equipo.
					12.1.1 Documentación de procedimientos operacionales.	Requerimientos para la documentación formal y comunicación al personal relevante.
					12.3.1 Respaldo de información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.				18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	13.2.4 Acuerdos de confidencialidad o de no divulgación.	Requerimientos para el diseño e implementación de acuerdos de confidencialidad y de no divulgación que reflejen las necesidades de la organización en cuento a protección de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
					6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
					7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
					8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
					9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
					10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
					12 Seguridad en las operaciones	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
					13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
					14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
					15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
					16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
					17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
					8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
					14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal	Actividades para prevenir brechas relacionadas a la seguridad de información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Identificable.	personal
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	5.1.1 Políticas de Seguridad de la Información.	Actividades y requerimientos para definir un set de políticas relacionadas a la seguridad de la información
					6.2.1 Política de Dispositivos Móviles.	Lineamientos para la implementación de una política para el uso y protección de medios móviles.
					7.2.3 Proceso disciplinario.	Actividades para el establecimiento de un proceso disciplinario en caso de violaciones a la seguridad de la información.
					8.1.3 Uso aceptable de activos.	Establecimiento formal de reglas para el uso aceptable de activos de información.
					9.1.1 Política de Control de Acceso.	Lineamientos para el establecimiento de una política de control de acceso a la información.
					10.1.1 Política sobre el uso de controles criptográficos.	Aspectos relevantes para el desarrollo de una política sobre el uso de controles criptográficos para protección de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					11.2.9 Política de escritorio y pantalla limpios.	Lineamientos para la implementación de una política de escritorio y pantalla limpios.
					13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
					14.2.1 Política de desarrollo seguro.	Establecimiento formal de políticas de seguridad para el desarrollo de software.
					15.1.1 Política de Seguridad de la Información para el relacionamiento con terceros.	Guía para el establecimiento formal de requerimientos de seguridad cuando se trabaja con proveedores.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Información.	seguridad de la información.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
					18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.
					18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
					18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.1. Dirección de la Gerencia para Seguridad de la Información.	Las actividades para proveer dirección y soporte para la seguridad de la información de acuerdo a los requerimientos del negocio.
					6.1 Organización interna.	Actividades para el establecimiento de un marco para iniciar y controlar la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						operación de la seguridad de la información.
					18.1 Cumplimiento con requerimientos legales y contractuales.	Actividades para prevenir brechas en cuanto a regulaciones, requerimientos legales, y contractuales.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
					8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
					14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
					18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
					18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
					18.2.1 Revisión independiente de Seguridad de la Información.	La organización debe someterse a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.
					18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
					18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	12.1.1 Documentación de procedimientos operacionales.	Lineamientos de documentación de procedimientos operacionales y su difusión a las partes relevantes.
					16.1 Gestión de incidentes y mejoras de Seguridad de la Información.	Actividades para la administración de incidentes de seguridad.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	7.2.3 Proceso disciplinario.	Actividades para el establecimiento de un proceso disciplinario en caso de violaciones a la seguridad de la información.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información para un ISMS.
					6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
					7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
					9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
					10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
					11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
					12 Seguridad en las Operaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
					13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
					14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
					15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
					17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.
					18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.3.1 Gestión de medios removibles.	Lineamientos para la implementación de procedimientos para la gestión de medios removibles.
					8.3.2 Eliminación de medios.	Requerimientos para la disposición de medios de forma segura cuando estos ya no sean utilizados.
					12.7.1 Controles de auditoría sistemas de información.	Actividades para la ejecución de auditorías con el objetivo de minimizar interrupciones en los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
					14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.1.1 Roles y responsabilidades de Seguridad de la Información.	Todas los roles y responsabilidades deben ser definidos y asignados.
					7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la Información.	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la seguridad de la información.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de	5 Políticas de Seguridad de la Información.	Recomendaciones para el establecimiento de políticas de seguridad de la información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.			seguridad y Análisis de Brecha.		para un ISMS.
					6 Organización de Seguridad de la Información.	Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
					7 Seguridad de Recursos Humanos.	Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
					8 Gestión de Activos.	Actividades para el control de activos de información dentro del alcance de un ISMS.
					9 Control de Acceso.	Prácticas para el control de acceso a los activos de información o información dentro del alcance de un ISMS.
					10 Criptografía.	Lineamientos para la protección de la información por medios criptográficos.
					11 Seguridad Física y Ambiental.	Actividades para la prevención de eventos que pueden dañar los activos de información.
					12 Seguridad en las operaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						procesamiento.
					13 Seguridad en las Comunicaciones.	Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
					14 Adquisición, desarrollo y mantenimiento de Sistemas.	Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas.
					15 Relacionamiento con los Proveedores.	Prácticas para la administración de la seguridad de la información con proveedores.
					16 Gestión de Incidentes de Seguridad de la Información.	Actividades para la gestión de incidentes de seguridad de la información.
					17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.	Actividades para el establecimiento de un plan de continuidad del negocio.
					18 Cumplimiento.	Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
					8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
					14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	8.1.1 Inventario de activos.	Todos los activos asociados con información e infraestructura de procesamiento deberán de estar identificados en un inventario,
					8.1.2 Propiedad de activos.	Todos los activos de información identificados deben tener asignado un dueño que será responsable de los mismos.
					8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
					8.2.2 Etiquetado de información.	Establece los requerimientos para el etiquetado de información de acuerdo a su clasificación.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.1.1 Políticas de Seguridad de la Información.	Actividades y requerimientos para definir un set de políticas relacionadas a la seguridad de la información
					6.1.1 Roles y responsabilidades de	Todas los roles y responsabilidades deben ser

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Seguridad de la Información.	definidos y asignados.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1.5 Seguridad de la Información en la Gestión de Proyectos.	Actividades para la administración de la seguridad en proyectos.
					8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
					14.1.1 Análisis y especificación de requerimientos de Seguridad de la Información.	Lineamientos para la inclusión de requerimientos de seguridad para la adquisición, desarrollo o mejoras en los sistemas existentes.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal.
					18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
					18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma operativa.	Actividades para asegurar que no hay efectos negativos después de haberse realizado cambios en las plataformas operativas.
					18.2 Revisiones de Seguridad de la Información.	Actividades para asegurar que la seguridad de la información se encuentra implementada y operando de acuerdo a las políticas y procedimientos establecidos.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	12.6.1 Gestión de vulnerabilidades técnicas.	Actividades para identificar y prevenir que las vulnerabilidades técnicas en los activos de información sean explotadas.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,
					18.2.1 Revisión	La organización debe someterse

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					independiente de Seguridad de la Información.	a revisiones independientes de seguridad de la información en intervalos planeados o cuando ocurran cambios significativos.
					18.2.2 Cumplimiento con políticas y estándares de Seguridad.	La dirección debe evaluar periódicamente el nivel de cumplimiento respecto a políticas y procedimientos de seguridad de la información.
					18.2.3 Revisión de cumplimiento técnico.	Revisiones periódicas sobre el cumplimiento de los sistemas de información de acuerdo a las políticas establecidas.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.2.2 Concienciación, Educación, y Entrenamiento de Seguridad de la Información.	Actividades para desarrollar e implementar un programa de entrenamiento y capacitación sobre temas relevantes para la seguridad de la información.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.1.1 Inventario de activos.	Todos los activos asociados con información e infraestructura de procesamiento deberán de estar identificados en un inventario,
					8.1.2 Propiedad de activos.	Todos los activos de información identificados deben tener asignado un dueño que

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						será responsable de los mismos.
					8.2.1 Clasificación de Información.	Lineamientos para la clasificación de información de la organización.
					8.2.2 Etiquetado de información.	Establece los requerimientos para el etiquetado de información de acuerdo a su clasificación.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	8.1.1 Inventario de activos.	Todos los activos asociados con información e infraestructura de procesamiento deberán de estar identificados en un inventario,
					8.1.2 Propiedad de activos.	Todos los activos de información identificados deben tener asignado un dueño que será responsable de los mismos.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad		Art. 62	Paso 8. Revisiones y Auditoría.	5.1.2 Revisión de las políticas de Seguridad de la Información.	Las políticas de seguridad de la información deberán ser revisadas por la dirección o en caso de algún cambio relevante en la organización,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	16.1 Gestión de incidentes y mejoras de Seguridad de la Información.	Actividades para la administración de incidentes de seguridad.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	16.1.5 Respuesta a incidentes de Seguridad de la Información.	Procedimientos para la respuesta a incidentes de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	16.1.6 Lecciones aprendidas de los incidentes de Seguridad de la Información.	Establecimiento de una base de datos de eventos de seguridad para minimizar el impacto de eventos similares en el futuro.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50	1. Recomendación General.	13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.
					15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
					15.2 Gestión de la entrega de servicios de proveedores.	Actividades para el mantenimiento de niveles de servicio y seguridad apropiados con terceras partes.
					18.1 Cumplimiento con requerimientos legales y contractuales.	Lineamientos para prevenir relacionadas a layes y regulaciones o contratos relacionados a seguridad de la información
SUBCONTRATACIONES						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
					13.2.4 Acuerdos de confidencialidad o de no divulgación.	Requerimientos para el diseño e implementación de acuerdos de confidencialidad y de no divulgación que reflejen las necesidades de la organización en cuento a protección de información.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
					18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
					13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
					13.2.4 Acuerdos de confidencialidad o de no divulgación.	Requerimientos para el diseño e implementación de acuerdos de confidencialidad y de no divulgación que reflejen las necesidades de la organización en cuento a protección de información.
					15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
					15.2 Gestión de la entrega de servicios de proveedores.	Actividades para el mantenimiento de niveles de servicio y seguridad apropiados con terceras partes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos personales sobre los que se preste el servicio.				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.
					15.1 Seguridad de la Información para el relacionamiento con proveedores.	Actividades para asegurar la protección de los activos de información que esta accesible para terceros.
					15.2 Gestión de la entrega de servicios de proveedores.	Actividades para el mantenimiento de niveles de servicio y seguridad apropiados con terceras partes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	13.2 Transferencia de información.	Actividades para mantener la seguridad en la información transmitida dentro de la organización y entidades externas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	18.1.1 Identificación de legislación aplicable y requerimientos contractuales.	Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
					18.1.3 Protección de registros.	Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
					18.1.4 Privacidad y protección de Información Personal Identificable.	Actividades para prevenir brechas relacionadas a la seguridad de información personal
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
					13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
					13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	13.2.1 Políticas y procedimientos de transferencia de información.	Actividades para el desarrollo de la política y procedimientos de transferencia de información.
					13.2.2 Acuerdos sobre transferencia de información.	Lineamientos para establecer acuerdos de información entre la organización y entidades externas.

4.3 ISO/IEC 27005:2008, Information Technology - Security techniques – Information security risk management.

Introducción. Este estándar proporciona lineamientos para la gestión de riesgos de seguridad de la información. Su finalidad es apoyar la implementación de seguridad de la información con base en un enfoque de gestión de los riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	7 Establecimiento del Contexto.	Información de la organización que sea relevante para el establecimiento de la gestión de riesgos de seguridad de la información.
					8 Evaluación del Riesgo de Seguridad de la Información.	Actividades para la identificación, evaluación, y priorización de los riesgos de seguridad de la información.
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
					10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
					12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.					
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
			INFORMACIÓN			
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
			FINALIDAD			
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
			PROPORCIONALIDAD			
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
			CONFIDENCIALIDAD			
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titular o, en su caso, con el responsable.					
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	7 Establecimiento del Contexto.	Información de la organización que sea relevante para el establecimiento de la gestión de riesgos de seguridad de la información
					8 Evaluación del Riesgo de Seguridad de la Información.	Actividades para la identificación, evaluación, y priorización de los riesgos de seguridad de la información.
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
					10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
					11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
					12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	7.1 Consideraciones generales.	Factores de la organización que inciden en la gestión de riesgos de seguridad de la información.
					7.2 Criterios básicos.	Establecimiento de criterios y enfoque para la gestión de seguridad de la información.
					8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
					8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
					8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	12 Monitoreo y revisión de Riesgos de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
					12.1 Monitoreo y revisión de factores de riesgo.	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
					12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	7.2 Criterios básicos.	Establecimiento de criterios y enfoque para la gestión de seguridad de la información.
					7.3 Límites y alcance.	Factores a considerar para la definición de límites y alcance de la gestión de seguridad de la información.
					7.4 Organización para la Gestión del Riesgo de Seguridad de la	Organización y responsabilidades para la gestión del riesgo de seguridad

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Información.	de la información.
					8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
					8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
					8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
					10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
					11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	12 Monitoreo y revisión de Riesgos de Seguridad de la Información	Acciones para monitorear los riesgos y sus factores en la organización.
					12.1 Monitoreo y revisión de factores de riesgo	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
					12.2 Monitoreo, revisión, y mejora de la gestión del riesgo	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá	Art. 19	Art. 4 Art. 9	Paso 6. Identificación de las	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.		Art. 57	medidas de seguridad y Análisis de Brecha.		
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	7.2 Criterios básicos.	Establecimiento de criterios y enfoque para la gestión de seguridad de la información.
					7.3 Límites y alcance.	Factores a considerar para la definición de límites y alcance de la gestión de seguridad de la información.
					7.4 Organización para la Gestión del Riesgo de Seguridad de la Información.	Organización y responsabilidades para la gestión del riesgo de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
					8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.
					8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información
					10 Aceptación del Riesgo de Seguridad de la Información	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
					12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	8.2.2 Identificación de activos	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.2 Identificación del Riesgo.	Identificación de las fuentes de riesgo aplicables a la organización.
					8.3 Análisis del Riesgo.	Actividades para la conducción de un análisis de riesgos de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
					10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
					11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
					12 Monitoreo y revisión del Riesgo de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.2.2 Identificación de activos.	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información.
					8.2.3 Identificación de amenazas.	Identificación de amenazas aplicables a la organización y su probabilidad de ocurrencia.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.2.4 Identificación de controles existentes.	Identificación y documentación de controles existentes incluyendo su efectividad.
					8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
					8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
					8.3.2 Evaluación de consecuencias.	Identificación de escenarios de impacto al negocio por incidentes de seguridad.
					8.3.3 Evaluación de probabilidad de incidente.	Determinación de la probabilidad de un incidente de seguridad.
					8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9 Tratamiento del Riesgo de Seguridad de la Información.	Acciones para reducir, evitar, transferir, aceptar los riesgos de seguridad de la información.
					10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.2.2 Identificación de activos	Proceso de identificación de los activos para facilitar el análisis de riesgos de seguridad de la información
					8.2.3 Identificación de amenazas.	Identificación de amenazas aplicables a la organización y su probabilidad de ocurrencia.
					8.2.4 Identificación de controles existentes.	Identificación y documentación de controles existentes incluyendo su efectividad.
					8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
					8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						organización.
					8.3.2 Evaluación de consecuencias.	Identificación de escenarios de impacto al negocio por incidentes de seguridad
					8.3.3 Evaluación de probabilidad de incidente.	Determinación de la probabilidad de un incidente de seguridad.
					8.4 Evaluación del Riesgo.	Actividades para llevar a cabo decisiones sobre los riesgos de seguridad de la información tomando en cuenta el contexto de la organización.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	9.1 Descripción general del Tratamiento del Riesgo.	Lineamientos para el tratamiento del riesgo.
					9.2 Modificación del Riesgo.	Medidas para modificar el riesgo.
					9.3 Retención del Riesgo.	Lineamientos para la retención del riesgo.
					9.4 Cancelación del Riesgo.	Lineamientos para la cancelación del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.5 Transferencia del Riesgo.	Lineamientos para la trasferencia del riesgo.
					10 Aceptación del Riesgo de Seguridad de la Información.	Acciones para decidir la aceptación de los riesgos resultantes de seguridad de la información.
					11 Comunicación y Consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	12 Monitoreo y revisión de Riesgos de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
					12.1 Monitoreo y revisión de factores de riesgo.	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
					12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo	8.2.2 Identificación de activos.	Proceso de identificación de los activos para facilitar el análisis

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				de los Datos Personales.		de riesgos de seguridad de la información.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	8.2.4 Identificación de controles existentes.	Identificación y documentación de controles existentes incluyendo su efectividad.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	12 Monitoreo y revisión de Riesgos de Seguridad de la Información.	Acciones para monitorear los riesgos y sus factores en la organización.
					12.1 Monitoreo y revisión de factores de riesgo.	Actividades para el monitoreo y revisión de los factores de riesgo en la organización.
					12.2 Monitoreo, revisión, y mejora de la gestión del riesgo.	Actividades para determinar lo adecuado y efectivo de la gestión del riesgo en la organización.
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
					8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
					8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	información al respecto.					
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	8.2.5 Identificación de vulnerabilidades.	Consideraciones para identificar las vulnerabilidades que pueden ser explotadas en la organización.
					8.2.6 Identificación de consecuencias.	Consideraciones para identificar las consecuencias de las vulnerabilidades en términos de la integridad, confidencialidad, y disponibilidad de los activos de información de la organización.
					8.3.2 Evaluación de consecuencias.	Identificación de escenarios de impacto al negocio por incidentes de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50	1. Recomendación General.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
SUBCONTRATACIONES						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable corresponderá al encargado.					
	CÓMPUTO EN LA NUBE					
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos personales sobre los que se preste el servicio.					
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
	TRANSFERENCIAS					
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	7.2.1 Enfoque de la Gestión del Riesgo.	Desarrollo de un enfoque de la gestión del riesgo para abordar los criterios de evaluación, impacto, y aceptación de riesgos.
					7.2.2 Criterios de evaluación del Riesgo.	Factores de la organización a considerar para la evaluación del riesgo.
					7.2.3 Criterio para el Impacto.	Factores de la organización a considerar para determinar el impacto de los riesgos.
					7.2.4 Criterio para aceptación del Riesgo.	Definición de escalas y niveles de aceptación del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					11 Comunicación y consulta del Riesgo de Seguridad de la Información.	Acciones para comunicar los riesgos de la organización a las partes interesadas.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

4.4 ISO/IEC 27006:2011, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.

Introducción. Este estándar establece los requerimientos y es una guía para entidades que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información. Su enfoque principal es para ayudar a la acreditación de entidades de certificación de sistemas de gestión de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	RESPONSABLE					
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de la Información.	
	LICITUD Y LEALTAD					
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
	CONSENTIMIENTO					
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
	INFORMACIÓN					
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.			Personales.		
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.			Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad		
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
	CALIDAD					
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados,	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.					
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
	FINALIDAD					

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
	PROPORCIONALIDAD					
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
	CONFIDENCIALIDAD					
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	RESPONSABILIDAD					
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de		Art. 48 - III	Paso 8. Revisiones y Auditoría.	9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	las políticas de privacidad.				9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.
					9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
					9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
					9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
					9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	7.1.1.1 Análisis de competencias y revisión contractual.	Establece el proceso de revisión de la organización cliente en cuanto a sus riesgos y su competencia en seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.
					9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.
					9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
					9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
					9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
					9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría especial.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
	SEGURIDAD					

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	9.2.3.3.1 Cumplimiento legal y regulatorio.	Establece la responsabilidad del cumplimiento legal y regulatorio.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.					
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	9.1.1.1 Criterios de auditoría de certificación.	Establece como criterio de auditoría al utilizado en ISO 27001.
					9.1.2 Alcance de la certificación.	Define el alcance con el cual se realizará la auditoría para la organización incluyendo sus riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9.1.5 Metodología de auditoría.	Requiere el uso de procedimientos para ejecutar la auditoría.
					9.1.6 Reporte de auditoría de certificación.	Describe los elementos que componen un reporte de auditoría de certificación.
					9.2.3.1 Auditoría Etapa 1.	Revisión del diseño del sistema de gestión.
					9.2.3.2 Auditoría Etapa 2.	Define la auditoría en sitio del sistema de gestión.
					9.3 Actividades de supervisión.	Describe las actividades de supervisión y seguimiento para el mantenimiento del sistema de gestión.
					9.3.1 Auditorías de supervisión.	Define las auditorías de supervisión y mantenimiento del sistema de gestión.
					9.4 Recertificación.	Describe las circunstancias y condiciones para mantener la certificación.
					9.4.1 Auditorías de recertificación.	Condiciones para responder a las no conformidades.
					9.5 Auditorías especiales.	Describe las circunstancias y condiciones para una auditoría especial.
					9.5.1 Casos especiales.	Define a los cambios mayores en el sistema de gestión para llevar a cabo una auditoría

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						especial.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento.		Art. 62	Paso 8. Revisiones y Auditoría.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					
	VULNERACIONES A LA SEGURIDAD					
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	información al respecto.					
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
	ENCARGADO					
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad		Art. 50	1. Recomendación General.	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
	SUBCONTRATACIONES					
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
	CÓMPUTO EN LA NUBE					
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8.5 Confidencialidad.	Establece la protección de registros confidenciales del sistema de gestión.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Cumplimiento Cotidiano de Medidas de Seguridad.		
	TRANSFERENCIAS					

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	10.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información.	Recomienda la implementación del sistema de gestión con base en ISO 27001.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8.6 Intercambio de información entre el ente certificador y sus clientes.	Consideraciones para proteger la información que se intercambia entre el ente certificador y la organización cliente.

4.5 ISO/IEC TR 27008:2011, Information technology -- Security techniques -- Guidelines for auditors on information security controls.

Introducción. Este estándar es una guía para la revisión de la implementación y operación de controles, incluyendo la revisión del cumplimiento técnico de controles de sistemas de información, en concordancia con los estándares de seguridad de la información establecidos en la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba		Art. 20	Paso 7. Implementación de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	recaerá, en todos los casos, en el responsable.			las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.					
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
					8.2.5 Hallazgos previos.	Consideraciones del uso de hallazgos previos para la revisión de controles.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.					
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	NO APLICA	NO APLICA
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales.			de Brecha.	7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad		Art. 61 - VI	Paso 7. Implementación de	8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	faltantes, derivadas del análisis de brecha.			las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.		
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						mantenimiento.
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	8.1 Preparaciones	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento
					8.2.4 Consideraciones relacionadas a los objetos	Especificación, documentación, y configuración de activos de información y la selección de los métodos de revisión apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.2.7 Sistemas externos	Revisión de sistemas de información externos a la organización
					8.2.8 Organización y activos de información	Adaptación de los procesos de revisión para sistemas y plataformas específicas
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	7 Métodos de Revisión.	Conceptos básicos de revisión de controles incluyendo procedimientos, reporte, y seguimiento.
					7.2 Examinación.	Proceso de inspección y análisis de objetos sujetos de revisión.
					7.3 Entrevista.	Proceso de entrevistas para el entendimiento, aclaración, o localización de evidencia.
					7.4 Prueba.	Proceso de prueba de los objetos sujetos a revisión para determinar su existencia y efectividad.
					8 Actividades.	Actividades de preparación de los controles para su revisión.
					8.1 Preparaciones.	Preparación de políticas y controles para su revisión incluyendo a los responsables de su operación y mantenimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.2 Desarrollo de un plan.	Actividades para desarrollar un plan de revisión incluyendo el enfoque y tipo de la misma.
					8.3 Ejecutar revisiones.	Aplicación de métodos de revisión para la inspección de los objetos sujetos de revisión.
					8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	forma inmediata. V. Los medios donde puede obtener más información al respecto.					
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	8.4 Análisis y reporte de resultados.	Actividades y componentes del reporte de la revisión.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad		Art. 50	1. Recomendación General.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Medidas de Seguridad.		
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Seguridad.		
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	NO APLICA	NO APLICA
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

4.6 ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.

Introducción. Este estándar internacional provee una estructura general para la protección de información de identificación personal (PII: Personally Identifiable Information). Con el estándar ISO 29100 se pretende ayudar a las organizaciones a definir los mecanismos de protección relacionados a la privacidad de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	4 Elementos básicos del marco de trabajo de Privacidad.	Describe los componentes básicos relacionados a la privacidad de datos personales para el establecimiento del marco de privacidad.
					5 Los principios de Privacidad de ISO/IEC 29100.	Describe a detalle los principios que deben ser utilizados para el desarrollo de políticas y procedimientos utilizados para la protección de datos personales.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.				5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
					5.4 Límite en la recolección.	Indica las limitantes para la recopilación de datos personales.
					5.5 Minimización de datos.	Define cómo deben ser divulgados los datos personales bajo el principio de la necesidad de saber.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						que serán obtenidos.
					5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	4.4.7 Información Personal Identificable Sensible.	Características de la información personal sensible de acuerdo al estándar.
					5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
			INFORMACIÓN			
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
					5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
					5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
					5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.8 Apertura, transparencia y aviso.	Principio que se refiere a la transparencia hacia el titular sobre el tratamiento y propósito de la recolección de sus datos personales.
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	5.7 Precisión y calidad.	Este principio establece que los datos recopilados deben ser exactos, completos y actualizados de acuerdo al

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	para el cumplimiento de la finalidad para la cual son tratados.					propósito para el que sean recopilados.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
					4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por las relaciones contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
					4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
					5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
FINALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
					5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
					5.4 Límite en la recolección.	Indica las limitantes para la recopilación de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.5 Minimización de datos.	Define cómo deben ser divulgados los datos personales bajo el principio de la necesidad de saber.
					5.6 Límites en el uso, retención, y eliminación.	Trata sobre la retención, uso, divulgación, transferencia y eliminación de acuerdo al propósito para el que fueron recopilados.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular,	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.					
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.5 Requerimientos de protección de la Privacidad.	Provee una definición de los requerimientos de protección de datos personales y los factores que influyen en ellos.
					4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	4.6 Políticas de Privacidad.	Elementos para el diseño y establecimiento de la política de privacidad de una organización.
					5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.5 Requerimientos de protección de la Privacidad.	Provee una definición de los requerimientos de protección de datos personales y los factores que influyen en ellos.
					4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.9 Acceso y participación individual.	Hace referencia a los derechos del titular sobre sus datos personales después de haber sido recopilados por el responsable.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
					5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.				5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.					
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo	5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				para la Implementación de las Medidas de Seguridad Faltantes.		
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	4.7 Controles de Privacidad.	Definir controles de privacidad con base en un análisis de riesgos e identificación de amenazas.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una		Art. 62	Paso 8. Revisiones y Auditoría.	5.12 Cumplimiento de la Privacidad.	Actividades para determinar que las acciones implementados logran los objetivos de protección de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	vez al año.					
			VULNERACIONES A LA SEGURIDAD			
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.		Art. 50	1. Recomendación General.	4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
					4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.
					4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
					4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					personales pueden ser afectados por las relaciones contractuales.
					4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
					4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que		Art. 51	Paso 7. Implementación de las Medidas de Seguridad	4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	permita acreditar su existencia, alcance y contenido.			Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		encuentre la compañía.
					4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por las relaciones contractuales.
					4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
					4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
					4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.
					4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
					4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por las relaciones

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						contractuales.
					4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
					4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.
					4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se encuentre la compañía.
					4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por las relaciones contractuales.
					4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.2.4 Terceros.	Describe las características de un tercero en relación a datos personales.
					4.3 Interacciones.	Describe los escenarios en los que los datos personales pueden ser tratados para determinar niveles de responsabilidad.
					4.5.1 Factores legales y regulatorios.	Establece que se deben de tomar en cuenta leyes y regulaciones legales de acuerdo a la localidad donde se

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					encuentre la compañía.
					4.5.2 Factores contractuales.	Indica que los requerimientos para el resguardo de datos personales pueden ser afectados por las relaciones contractuales.
					4.5.3 Factores de negocio.	Las medidas de seguridad sobre los datos personales pueden variar por factores propios del negocio.
					4.5.4 Otros factores.	Provee algunos otros factores que pueden afectar la definición de medidas de seguridad relacionadas a privacidad de datos.
					5.11 Seguridad de la Información.	Principio orientado a proveer integridad, disponibilidad y disponibilidad de datos personales.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.2 Opción y consentimiento.	Describe cómo deben ser presentados los principios de opción y consentimiento al dueño de los datos personales que serán obtenidos.
					5.3 Propósito legítimo y especificación.	Referente a la especificación del propósito y la legitimidad del mismo ante la recopilación de datos personales.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	4 Elementos básicos del marco de trabajo de Privacidad.	Describe los componentes básicos relacionados a la privacidad de datos personales para el establecimiento del marco de privacidad.
					5 Los principios de Privacidad de ISO/IEC 29100.	Describe a detalle los principios que deben ser utilizados para el desarrollo de políticas y procedimientos utilizados para la protección de datos personales.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.10 Responsabilidad.	Establece los parámetros de responsabilidad sobre el tratamiento de datos personales.

4.7 ISO/IEC 20000-1:2011 Information technology - Service management -Part 1: Service management system requirements.

Introducción. ISO 20000 es un estándar orientado al establecimiento de procesos y procedimientos para la gestión de servicios de TI y con ello prevenir los riesgos tecnológicos dentro de la operación de una organización. La gestión de los servicios de tecnología informática es un enfoque integrado basado en procesos que alinea la prestación de servicios de TI con las necesidades de la organización que los presta.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	4.1 Responsabilidad de la Gerencia.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.
					4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					4.3 Gestión de documentación.	El proveedor del servicio debe establecer y mantener los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						documentos, incluyendo los registros, para asegurar la eficaz planificación, operación y control del sistema de gestión de servicios.
					4.4 Gestión de Recursos.	El proveedor de servicios debe determinar y proporcionar los recursos humanos, técnicos, informativos y financieros necesarios.
					4.5 Establecer y mejorar el Sistema de Gestión de Servicios.	El proveedor de servicios debe definir e incluir el alcance del sistema de gestión de servicios en el plan de gestión de servicios.
					5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
					6 Procesos de Entrega de Servicios.	El proveedor de servicios deberá estar de acuerdo a los servicios que se entregarán con el cliente.
					7 Procesos de Relacionamiento.	El proveedor de servicios deberá identificar y documentar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						los clientes, usuarios y partes interesadas de los servicios.
					8 Procesos de Resolución.	Habrá un procedimiento documentado para todas las incidencias.
					9 Procesos de Control.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.					importante en los servicios o la atención al cliente.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el		Art. 20	Paso 7. Implementación de las Medidas de	4.3.3 Control de registros.	Se deberán mantener registros para demostrar la conformidad con los requisitos así como el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	responsable.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		buen funcionamiento del sistema de gestión de servicios.
					5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	4.3.3 Control de registros.	Se deberán mantener registros para demostrar la conformidad con los requisitos así como el buen funcionamiento del sistema de gestión de servicios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiado.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						gestión de la relación, el contrato y el rendimiento del proveedor.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	4.1 Responsabilidad de la Gerencia.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.
					4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					4.3 Gestión de documentación.	El proveedor del servicio debe establecer y mantener los documentos, incluyendo los registros, para asegurar la eficaz planificación, operación y control del sistema de gestión de servicios.
					4.4 Gestión de Recursos.	El proveedor de servicios debe determinar y proporcionar los recursos humanos, técnicos, informativos y financieros

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						necesarios.
					4.5 Establecer y mejorar el Sistema de Gestión de Servicios.	El proveedor de servicios debe definir e incluir el alcance del sistema de gestión de servicios en el plan de gestión de servicios.
					5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
					6 Procesos de Entrega de Servicios.	El proveedor de servicios deberá estar de acuerdo a los servicios que se entregarán con el cliente.
					7 Procesos de Relacionamiento.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
					8 Procesos de Resolución.	Habrá un procedimiento documentado para todas las incidencias.
					9 Procesos de Control.	Habrá una definición documentada de cada tipo de elemento de configuración. La

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información registrada para cada elemento de configuración garantizará el control.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	4.4.2 Recursos Humanos.	El personal del proveedor de servicios que realice trabajos que afecten la conformidad con los requisitos de servicio debe ser competente con base en la educación, formación, habilidades y experiencia.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					4.5.4 Monitoreo y revisión del Sistema de Gestión de Servicios.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	4.4.1 Provisión de Recursos.	El proveedor de servicios debe determinar y proporcionar los recursos humanos, técnicos, informativos y financieros necesarios.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						prioridad a los riesgos de seguridad de la información.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
					8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	4.1 Responsabilidad de la Gerencia.	La gerencia debe proporcionar evidencia de su compromiso con la planificación, establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de servicios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						garantizará el control.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.1.4 Representante de la Gerencia.	La gerencia debe designar un miembro de la gerencia del proveedor de servicios que, con independencia de otras responsabilidades, tiene las facultades y responsabilidades que incluyen los procesos del sistema de gestión de servicios.
					7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.					
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	5 Diseño y transición de servicios nuevos y cambiados.	El proveedor de servicios deberá utilizar este proceso para todos los nuevos servicios y cambios a los servicios con el potencial de tener un impacto importante en los servicios o la atención al cliente.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiada.
					4.4.2 Recursos Humanos.	El personal del proveedor de servicios que realice trabajos que afecten la conformidad con los requisitos de servicio debe ser competente con base en la educación, formación, habilidades y experiencia.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.5.4 Monitoreo y revisión del Sistema de Gestión del Servicio.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	4.5.4 Monitoreo y revisión del Sistema de Gestión del Servicio.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	4.1.2 Política de Gestión del Servicio.	La alta dirección debe asegurarse de que la política de gestión del servicio es apropiada.
					4.4.2 Recursos Humanos.	El personal del proveedor de servicios que realice trabajos que afecten la conformidad con los requisitos de servicio debe ser competente con base en la educación, formación, habilidades y experiencia.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	9.1 Gestión de la Configuración.	Habrá una definición documentada de cada tipo de elemento de configuración. La información registrada para cada elemento de configuración garantizará el control.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una		Art. 62	Paso 8. Revisiones y Auditoría.	4.5.4 Monitoreo y revisión del Sistema de Gestión del Servicio.	El proveedor de servicios deberá utilizar métodos adecuados para el seguimiento y la medición del sistema de gestión de servicios y los servicios.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	vez al año.					administrativos y técnicos.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8.1 Gestión de peticiones de incidentes y servicios.	Habrá un procedimiento documentado para todas las incidencias y para la gestión del cumplimiento de las solicitudes de servicio.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
					6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de seguridad de la información.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	6.6.3 Cambios e incidentes de Seguridad de la Información.	Incidentes de seguridad de la información, serán administrados mediante los procedimientos de gestión de incidentes, con una apropiada prioridad a los riesgos de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	efecto de evitar que la vulneración se repita.					seguridad de la información.
					8.2 Gestión de Problemas.	Habrá un procedimiento documentado para identificar los problemas y minimizar o evitar el impacto de los incidentes y problemas.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.		Art. 50	1. Recomendación General.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.			Cumplimiento Cotidiano de Medidas de Seguridad.	7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento;		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Cumplimiento Cotidiano de Medidas de Seguridad.	7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
					6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	7.1 Gestión de las relaciones de negocio.	El proveedor de servicios deberá identificar y documentar los clientes, usuarios y partes interesadas de los servicios.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.
					4.3.3 Control de registros.	Se deberán mantener registros para demostrar la conformidad con los requisitos así como el buen funcionamiento del sistema de gestión de servicios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	6.6.1 Política de Seguridad de la Información.	Gestión con apropiada autoridad aprobará una política de seguridad de la información, teniendo en cuenta los requisitos de servicio requisitos legales y reglamentarios y las obligaciones contractuales.
					6.6.2 Controles de Seguridad de la Información.	El proveedor de servicios deberá implementar y operar los controles de seguridad de información físicos, administrativos y técnicos.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4.2 Gobierno de procesos operados por otras partes.	El proveedor del servicio deberá demostrar la gobernabilidad de los procesos gestionados por un grupo interno, un cliente o un proveedor.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cumplimiento Cotidiano de Medidas de Seguridad.	7.2 Gestión de proveedores.	Para cada proveedor, el proveedor de servicios deberá tener una persona designada que es responsable de la gestión de la relación, el contrato y el rendimiento del proveedor.

4.8 ISO 22301:2012 Societal security - Business continuity management systems – Requirements.

Introducción. Este estándar especifica los requerimientos para planear, establecer, implementar, operar, supervisar, revisar, mantener, y mejorar de forma continua un sistema documentado de gestión para la protección contra eventos disruptivos en la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	4 Contexto de la Organización.	Factores internos y externos de la organización que afectan la implementación y operación de un sistema de gestión de la continuidad del negocio.
					5 Liderazgo.	Compromiso de la organización para la implementación y operación de un sistema de gestión de la continuidad del negocio.
					6 Planeación.	Establecimiento de objetivos de la continuidad del negocio y planeación de acciones para alcanzarlos.
					7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					8 Operación.	Procesos necesarios para la operación de un sistema de gestión de la continuidad del negocio.
					9 Evaluación de desempeño.	Actividades para el monitoreo, medición, análisis, y evaluación del desempeño de un sistema de gestión de la continuidad del negocio.
					10 Mejora.	Atención de no conformidades del sistema de gestión de la continuidad del negocio para su mejora continua.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba		Art. 20	Paso 7. Implementación de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	recaerá, en todos los casos, en el responsable.			las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.			las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	6.2 Objetivos de continuidad del negocio y planes para alcanzarlos.	Establecimiento de objetivos de continuidad del negocio así como de responsables para su consecución.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
					8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	7.5 Información documentada.	Documentación requerida y su manejo de conformidad con los requerimientos del sistema de gestión de continuidad del negocio.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	8.4 Establecimiento e implementación de procedimientos de continuidad del	Procedimientos y sus características para la implementación de los objetivos y planes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				negocio.	continuidad del negocio.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.2 Análisis de impacto al negocio y evaluación del riesgo.	Características de los procesos de análisis de impacto y evaluación del riesgo con respecto a la continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	5.3 Política.	Aspectos fundamentales que debe contener la política de continuidad del negocio de la organización.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.3 Concientización.	Concientización de todos los responsables de la organización para cumplir con los objetivos y planes de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					7.4 Comunicación.	Aspectos a considerar para el intercambio de información relacionada con el sistema de gestión de continuidad del negocio con las partes interesadas.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.
					9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
					9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
					7.1 Recursos.	Identificación de recursos necesarios para la implementación del sistema de gestión de continuidad del

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						negocio.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.2 Análisis de impacto al negocio y evaluación del riesgo.	Características de los procesos de análisis de impacto y evaluación del riesgo con respecto a la continuidad del negocio.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.
					9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
					9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cumplimiento Cotidiano de Medidas de Seguridad.		
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	5.1 Liderazgo y compromiso.	Responsabilidades en la organización para lograr los objetivos y planes de continuidad del negocio.
					5.2 Compromiso gerencial.	Responsabilidades de la gerencia para lograr los objetivos y planes de continuidad del negocio.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de	Procedimientos y sus características para la implementación de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					continuidad del negocio.	objetivos y planes de continuidad del negocio.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.4 Roles, responsabilidades, y autoridades organizacionales.	Asignación y comunicación de responsabilidades y autoridades dentro del sistema de gestión de continuidad del negocio.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.					
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.
					6.2 Objetivos de continuidad de negocio y planes para alcanzarlos.	Establecimiento de los objetivos de continuidad de negocio de la organización y determinación de acciones y responsables para lograr dichos objetivos.
					8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	5.4 Roles, responsabilidades, y autoridades organizacionales.	Asignación y comunicación de responsabilidades y autoridades dentro del sistema de gestión de continuidad del negocio.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.2 Análisis de impacto al negocio y evaluación del riesgo.	Características de los procesos de análisis de impacto y evaluación del riesgo con respecto a la continuidad del negocio.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis	8.4 Establecimiento e implementación de procedimientos de continuidad del	Procedimientos y sus características para la implementación de los objetivos y planes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales.			de Brecha.	negocio.	continuidad del negocio.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	10 Mejora.	Acciones para la mejora continua del sistema de gestión de continuidad del negocio.
					10.1 No conformidad y acciones correctivas.	Manejo de no conformidades detectadas en el sistema de gestión de continuidad del negocio.
					10.2 Mejora continua.	Proceso de mejora continua e implementación de correcciones al sistema de gestión de continuidad del negocio.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.
					9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
					9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						negocio.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	7.3 Concientización.	Concientización de todos los responsables de la organización para cumplir con los objetivos y planes de continuidad del negocio.
					7.4 Comunicación.	Aspectos a considerar para el intercambio de información relacionada con el sistema de gestión de continuidad del negocio con las partes interesadas.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	8.4 Establecimiento e implementación de procedimientos de continuidad del negocio.	Procedimientos y sus características para la implementación de los objetivos y planes de continuidad del negocio.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable.		Art. 62	Paso 8. Revisiones y Auditoría.	9.1 Monitoreo, medición, análisis y evaluación.	Aspectos específicos a considerarse en los procesos de monitoreo, medición, análisis, y evaluación del desempeño del sistema de gestión de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.				9.2 Auditoría interna.	Consideraciones para llevar a cabo la auditoría interna del sistema de gestión de continuidad del negocio.
					9.3 Revisión gerencial.	Actividades y elementos de la revisión gerencial al sistema de gestión de continuidad del negocio.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.					
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los		Art. 50	1. Recomendación General.	8.3 Estrategia de continuidad del negocio.	Requerimientos y aspectos para la determinación de la estrategia de continuidad del negocio.
					8.4 Establecimiento e implementación de procedimientos de continuidad del	Procedimientos y sus características para la implementación de los objetivos y planes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				negocio.	continuidad del negocio.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
					4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
					4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
					6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Cumplimiento Cotidiano de Medidas de Seguridad.	4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
					6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Cotidiano de Medidas de Seguridad.	4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
					6.1 Acciones para abordar los riesgos y las oportunidades.	Determinación de las acciones a llevar a cabo para abordar los riesgos y áreas de oportunidad de continuidad del negocio en la organización.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
					4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
					4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	4 Contexto de la Organización.	Factores internos y externos de la organización que afectan la implementación y operación de un sistema de gestión de la continuidad del negocio.
					5 Liderazgo.	Compromiso de la organización para la implementación y operación de un sistema de gestión de la continuidad del negocio.
					6 Planeación.	Establecimiento de objetivos de la continuidad del negocio y planeación de acciones para alcanzarlos.
					7 Soporte.	Componentes necesarios para la implementación de un sistema de gestión de la continuidad del negocio.
					8 Operación.	Procesos necesarios para la operación de un sistema de gestión de la continuidad del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					9 Evaluación de desempeño.	Actividades para el monitoreo, medición, análisis, y evaluación del desempeño de un sistema de gestión de la continuidad del negocio.
					10 Mejora.	Atención de no conformidades del sistema de gestión de la continuidad del negocio para su mejora continua.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.1 Entendimiento de la organización y su contexto.	Evaluación de los factores internos y externos que afectan a la organización para la implementación de un sistema de gestión de continuidad del negocio.
					4.2 Entendimiento de las necesidades y expectativas de las partes interesadas.	Actividades para el entendimiento de las necesidades y expectativas de las partes interesadas en el sistema de gestión de continuidad del negocio incluyendo aspectos regulatorios y legales.

4.9 ISO 31000:2009, Risk management – Principles and guidelines.

Introducción. Este estándar proporciona los principios y las guías genéricas para la gestión de riesgos, por lo que puede ser utilizada por cualquier organización no importando la industria o sector. Los puntos contenidos en este estándar pueden ser aplicados a lo largo de la vida de una organización, y para una diversidad de actividades, incluyendo estrategias y decisiones, operaciones, proceso, funciones, proyectos, productos, servicios, y activos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	RESPONSABLE					
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	2 Términos y definiciones.	Términos y definiciones de la gestión del riesgo.
					3 Principios.	Principios para la gestión efectiva del riesgo.
					4.2 Responsabilidad y compromiso.	Compromiso de la alta dirección de la organización para la gestión efectiva del riesgo.
					4.3 Diseño del marco de trabajo para la Gestión del Riesgo.	Características principales con las que debe contar un marco de trabajo para la gestión del riesgo.
					4.4 Implementación de la Gestión del Riesgo.	Consideraciones para la implementación efectiva de la gestión del riesgo.
					4.5 Monitoreo y revisión del marco de	Características de los procesos de monitoreo y revisión del

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					trabajo.	marco de trabajo de la gestión del riesgo.
					4.6 Mejora continua del marco de trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
					5.2 Comunicación y consulta.	Comunicación y consulta con las partes interesadas para la gestión efectiva del riesgo.
					5.3 Establecimiento del contexto.	Factores internos y externos a considerarse para la gestión efectiva del riesgo.
					5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
					5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
					5.6 Monitoreo y revisión.	Procesos de monitoreo y revisión del riesgo.
					5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.					
	CONSENTIMIENTO					
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.					
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática,	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.					
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	2.26 Control.	Definición y ejemplos de control.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	2.26 Control.	Definición y ejemplos de control.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.					
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	2.26 Control.	Definición y ejemplos de control.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	2.26 Control.	Definición y ejemplos de control.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.					
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	5.3 Estableciendo el contexto.	Factores internos y externos a considerarse para la gestión efectiva del riesgo.
					5.3.2 Contexto Externo.	Factores externos de la organización que inciden en la gestión del riesgo.
					5.3.3 Contexto Interno.	Factores internos de la organización que inciden en la gestión del riesgo.
					5.3.4 Estableciendo el contexto del proceso de Gestión del Riesgo.	Elementos necesarios para el establecimiento del contexto del proceso de gestión del riesgo.
					5.3.5 Definición de criterio del Riesgo.	Definición y establecimiento del criterio para evaluar el riesgo.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	4.3.2 Estableciendo la Política de Gestión del Riesgo.	Enfoque y elementos de la política de gestión del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
					4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
					5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.4.2 Identificación del Riesgo.	Actividades a considerar para la identificación del riesgo.
					5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
					5.4.4 Revisión del Riesgo.	Descripción general del proceso de revisión del riesgo.
					5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
					5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
					5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
					5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que		Art. 48 - IX	Paso 6. Identificación de las medidas de	5.5.2 Selección de opciones de Tratamiento del	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.			seguridad y Análisis de Brecha.	Riesgo.	tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
					5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
					5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
					5.4.2 Identificación del Riesgo.	Actividades a considerar para la identificación del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
					5.4.4 Revisión del Riesgo.	Descripción general del proceso de revisión del riesgo.
					5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
					5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	NO APLICA	NO APLICA
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	5.4 Evaluación del Riesgo.	Proceso de evaluación del riesgo y sus componentes.
					5.4.2 Identificación del Riesgo.	Actividades a considerar para la identificación del riesgo.
					5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
					5.4.4 Revisión del Riesgo.	Descripción general del proceso de revisión del riesgo.
					5.5 Tratamiento del Riesgo.	Selección de opciones y alternativas para modificación del riesgo.
					5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	5.4.3 Análisis del Riesgo.	Descripción general del proceso de análisis del riesgo.
					5.6 Monitoreo y revisión.	Procesos de monitoreo y revisión del riesgo.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de	5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				las Medidas de Seguridad Faltantes.		
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.
					4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
					5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
					5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales	2.26 Control.	Definición y ejemplos de control.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				documentadas.		
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	5.3 Estableciendo el contexto.	Factores internos y externos a considerarse para la gestión efectiva del riesgo.
					5.3.2 Contexto Externo.	Factores externos de la organización que inciden en la gestión del riesgo.
					5.3.3 Contexto Interno.	Factores internos de la organización que inciden en la gestión del riesgo.
					5.3.4 Estableciendo el contexto del proceso de Gestión del Riesgo.	Elementos necesarios para el establecimiento del contexto del proceso de gestión del riesgo.
					5.3.5 Definición de criterio del Riesgo.	Definición y establecimiento del criterio para evaluar el riesgo.
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas,		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la	4.5 Monitoreo y Revisión del Marco de Trabajo.	Características de los procesos de monitoreo y revisión del marco de trabajo de la gestión del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.			Información.	4.6 Mejora continua del Marco de Trabajo.	Acciones para llevar a cabo la mejora continua del marco de trabajo de la gestión del riesgo.
					5.6 Monitoreo y Revisión.	Procesos de monitoreo y revisión del riesgo.
					5.7 Registro del proceso de Gestión del Riesgo.	Acciones para llevar a cabo la trazabilidad de la gestión del riesgo.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación		Art. 50	1. Recomendación General.	5.5.2 Selección de opciones de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo.
					5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Características que deben ser consideradas en los planes de tratamiento del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.			Cotidiano de Medidas de Seguridad.		
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.					
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.5.2 Selección de opciones de Tratamiento del Riesgo. 5.5.3 Preparación e implementación de planes de Tratamiento del Riesgo.	Consideraciones a tomar en cuenta para la selección de opciones y alternativas de tratamiento del riesgo. Características que deben ser consideradas en los planes de tratamiento del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.					
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos		Art. 70	1. Recomendación General	4 Marco de Trabajo.	Aspectos del marco de trabajo para la gestión efectiva del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.				5 Proceso.	Procesos para la gestión efectiva del riesgo.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

4.10 ISO GUIDE 72, Guidelines for the justification and development of management systems standards.

Introducción. Esta guía proporciona los lineamientos para la justificación y evaluación de un proyecto estándar de un sistema de gestión incluyendo: la visión de la evaluación de relevancia en el mercado, los procesos de desarrollo y mantenimiento con una visión para asegurar su compatibilidad y mejora, y la terminología, estructura, y elementos comunes a ser integrados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	B1 Política.	Política para establecer el marco de trabajo para el establecimiento de objetivos y metas.
					B2 Planeación.	Procesos de planeación del sistema de gestión.
					B3 Implementación y Operación.	Procesos de implementación y operación del sistema de gestión.
					B4 Desempeño.	Procesos para la evaluación del desempeño del sistema de gestión.
					B5 Mejora.	Procesos para el mantenimiento y mejora continua del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					B6 Revisión Gerencial.	Proceso de revisión gerencial del sistema de gestión.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	B1.1 Política y Principios.	Política para demostrar el compromiso de la organización en el cumplimiento de los requerimientos del sistema de gestión.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	B1.1 Política y Principios.	Política para demostrar el compromiso de la organización en el cumplimiento de los requerimientos del sistema de gestión.
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes,	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.					identificados.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
					B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
					B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
					B2.7 Preparación de imprevistos para los acontecimientos previsibles.	Acuerdos necesarios para manejar emergencias previsibles.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
					B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
					B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	B1.1 Política y Principios.	Política para demostrar el compromiso de la organización en el cumplimiento de los requerimientos del sistema de gestión.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	B3.2 Gestión de recursos humanos.	Gestión de empleados, contratistas, terceros, entre otros, incluyendo revisión de sus cualidades y capacidades así como su entrenamiento.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
					B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
					B3.3 Gestión de otros recursos.	Gestión operacional y de mantenimiento de recursos que tienen un impacto en el desempeño de la organización.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
					B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
					B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
					B2.7 Preparación de imprevistos para los acontecimientos previsibles.	Acuerdos necesarios para manejar emergencias previsibles.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
					B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
					B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
					B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
					B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
					B2.6 Planeación de procesos operacionales Previsibles.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					B2.7 Preparación de imprevistos para los acontecimientos.	Acuerdos necesarios para manejar emergencias previsibles.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	B3.4 Documentación y su control.	Manejo de documentos que son esenciales para la implementación y operación exitosas del sistema de gestión.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	B2.5 Identificación de estructura organizacional, roles, responsabilidades, y autoridades.	Roles, responsabilidades, y sus interrelaciones dentro de la organización para la operación del sistema de gestión.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	B2.1 Identificación de necesidades, requerimientos y análisis de temas críticos.	Identificación de puntos que deben ser controlados y/o mejorados para satisfacer a las partes interesadas.
					B2.2 Selección de temas significantes a ser abordados.	Priorización de las necesidades y requerimientos identificados.
					B2.3 Identificación de objetivos y metas.	Identificación de objetivos y metas del sistema de gestión.
					B2.4 Identificación de recursos.	Identificación de recursos (humanos, financieros, de infraestructura) para el sistema de gestión.
					B2.5 Identificación de estructura	Roles, responsabilidades, y sus interrelaciones dentro de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					organizacional, roles, responsabilidades, y autoridades.	organización para la operación del sistema de gestión.
					B2.6 Planeación de procesos operacionales.	Planeación de acuerdos para los procesos operacionales a fin de lograr los objetivos y metas identificados.
					B2.7 Preparación de imprevistos para los acontecimientos previsibles.	Acuerdos necesarios para manejar emergencias previsibles.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	B3.1 Control Operacional.	Medidas necesarias de control operacional a ser implementadas para lograr los objetivos y metas del sistema de gestión.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo	B5.1 Acción correctiva.	Mecanismo para la eliminación de las causas de las no conformidades en el sistema de gestión.
					B5.2 Acción preventiva.	Mecanismos para eliminar las causas potenciales de las no conformidades en el sistema de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				para la Implementación de las Medidas de Seguridad Faltantes.		gestión.
					B5.3 Mejora continua.	Provisiones realizadas para la mejora continua del sistema de gestión.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
					B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
					B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	B3.2 Gestión de recursos humanos.	Gestión de empleados, contratistas, terceros, entre otros, incluyendo revisión de sus cualidades y capacidades así como su entrenamiento.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	B3.4 Documentación y su control.	Manejo de documentos que son esenciales para la implementación y operación exitosas del sistema de gestión.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la	B3.4 Documentación y su control.	Manejo de documentos que son esenciales para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				seguridad de los datos personales documentadas.		implementación y operación exitosas del sistema de gestión.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	B4.1 Monitoreo y medición.	Mecanismos por los cuales la organización mide su desempeño de una manera continua.
					B4.2 Análisis y manejo de no conformidades.	Determinación de no conformidades en el sistema de gestión y la forma en que son tratadas.
					B4.3 Auditorías del sistema.	Proceso de auditoría del sistema de gestión.
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	B3.5 Comunicación	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	B3.5 Comunicación.	Acuerdos para comunicar aspectos del sistema de gestión hacia fuentes externas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	efecto de evitar que la vulneración se repita.					
			ENCARGADO			
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la		Art. 50	1. Recomendación General.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.					
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio,		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.					
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
	TRANSFERENCIAS					
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	B1 Política.	Política para establecer el marco de trabajo para el establecimiento de objetivos y metas.
					B2 Planeación.	Procesos de planeación del sistema de gestión.
					B3 Implementación y Operación	Procesos de implementación y operación del sistema de gestión.
					B4 Desempeño.	Procesos para la evaluación del desempeño del sistema de gestión.
					B5 Mejora.	Procesos para el mantenimiento y mejora continua del sistema de gestión.
					B6 Revisión Gerencial.	Proceso de revisión gerencial del sistema de gestión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	B3.6 Relacionamiento con proveedores y contratistas.	Formalización de acuerdos entre quienes proveen y contratan servicios que tienen un impacto en el desempeño de la organización.

4.11 ISO GUIDE 73, Risk management – Vocabulary.

Introducción. El estándar proporciona las definiciones de los términos genéricos relacionados con la gestión del riesgo. El ISO Guide 73 promueve una base común de entendimiento y un enfoque coherente para la descripción de actividades y el uso uniforme de conceptos utilizados en procesos y marcos de trabajo para la gestión del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	2.1 Gestión del Riesgo.	Actividades para dirigir y controlar a una organización con respecto al riesgo.
					3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
					3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
					3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.
					3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.					
	CONSENTIMIENTO					
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.					
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática,	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.					
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	3.8.1.1 Control.	Medida para afectar el riesgo.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	3.8.1.1 Control.	Medida para afectar el riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.					
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	3.8.1.1 Control.	Medida para afectar el riesgo.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	3.8.1 Tratamiento del Riesgo. 3.8.1.1 Control.	Proceso para modificar el riesgo. Medida para afectar el riesgo.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular,	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	3.8.1.1 Control.	Medida para afectar el riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.					
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.3.1 Estableciendo el contexto.	Factores internos y externos para la gestión del riesgo.
					3.3.1.1 Contexto Externo.	Ambiente externo en el que la organización busca lograr sus objetivos.
					3.3.1.2 Contexto Interno.	Ambiente interno en el que la organización busca lograr sus objetivos.
					3.5.1.1 Descripción del Riesgo.	Definición estructurada del riesgo.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	2.1.2 Política de Gestión del Riesgo.	Declaración de cómo la organización gestiona el riesgo.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	3.8.2.6 Auditoría de Gestión del Riesgo.	Proceso para determinar si el marco de trabajo de gestión del riesgo es adecuado y efectivo.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Quienes Traten Datos Personales.		
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
					3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
					3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.
					3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo.
					3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	3.8.2.6 Auditoría de Gestión del Riesgo.	Proceso para determinar si el marco de trabajo de gestión del riesgo es adecuado y efectivo.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.
					3.8.1.6 Riesgo Residual.	Riesgo resultante después del tratamiento de riesgo.
					3.8.2.5 Perfil de Riesgo.	Descripción de un conjunto de riesgos.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
					3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
					3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo
					3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	NO APLICA	NO APLICA
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.4.1 Evaluación del Riesgo.	Proceso de identificación, análisis, y evaluación del riesgo.
					3.5.1 Identificación del Riesgo.	Proceso de encontrar, reconocer, y describir riesgos.
					3.6.1 Análisis del Riesgo.	Proceso de entender y determinar el nivel de riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					3.7.1 Evaluación del Riesgo.	Proceso para determinar la magnitud del riesgo.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.6.1.6 Vulnerabilidad.	Susceptibilidad a una fuente de riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.
					3.8.1.6 Riesgo Residual.	Riesgo resultante después del tratamiento de riesgo.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	2.1.3 Plan de Gestión de Riesgos.	Especifica el enfoque, componentes, y recursos para la gestión del riesgo.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	3.8.2.1 Monitoreo.	Supervisión del desempeño de la manera de gestionar el riesgo.
					3.8.2.2 Revisión.	Determinar lo adecuado y la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						efectividad de la gestión del riesgo.
					3.8.2.6 Auditoría de la Gestión del Riesgo.	Proceso independiente para determinar si el marco de trabajo de gestión del riesgo es adecuado y efectivo.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	3.8.1.1 Control.	Medida para afectar el riesgo.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de		Art. 62	Paso 8. Revisiones y Auditoría.	3.3.1 Estableciendo el contexto.	Factores internos y externos para la gestión del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.				3.3.1.1 Contexto Externo.	Ambiente externo en el que la organización busca lograr sus objetivos.
					3.3.1.2 Contexto Interno.	Ambiente interno en el que la organización busca lograr sus objetivos.
					3.8.2 Términos relacionados al monitoreo y medición.	Monitoreo y medición del riesgo.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3.8.2.1 Monitoreo.	Supervisión del desempeño de la manera de gestionar el riesgo.
					3.8.2.2 Revisión.	Determinar lo adecuado y la efectividad de la gestión del riesgo.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50	1. Recomendación General.	3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.
SUBCONTRATACIONES						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable corresponderá al encargado.					
	CÓMPUTO EN LA NUBE					
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos personales sobre los que se preste el servicio.					
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	3.8.1 Tratamiento del Riesgo.	Proceso para modificar el riesgo.
					3.8.1.1 Control.	Medida para afectar el riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
	TRANSFERENCIAS					
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	2.1.1 Marco de trabajo de Gestión del Riesgo.	Conjunto de componentes para el diseño, implementación, monitoreo, y seguimiento de la gestión del riesgo.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		

4.12 ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary.

Introducción. Es un documento de referencia para entender los términos y vocabulario relacionado con los sistemas de gestión de calidad. El ISO 9000:2005 está orientado a organizaciones que buscan tomar ventaja a través de la implementación de un sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	0.1 Generalidades.	Contexto de las normas ISO 9000 en la eficacia de los sistemas de gestión de la calidad.
					0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.
					1 Objeto y campo de aplicación.	Aplicabilidad de los sistemas de gestión de la calidad.
					2 Fundamentos de los Sistemas de Gestión de Calidad.	Fundamentos de los sistemas de gestión de la calidad para la satisfacción de los clientes.
					3 Términos y definiciones.	Conceptos base para el manejo de sistemas de gestión de la calidad.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y	Art. 7	Art. 7	Paso 1. Alcance y	2.5 Política de la	Documentos para proporcionar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.		Art. 10 Art. 44	Objetivos.	Calidad y objetivos de la Calidad.	un punto de referencia para dirigir la organización.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	2.7 Documentación	Aspectos de la documentación en los sistemas de gestión de la calidad
					2.7.1 Valor de la documentación	Contribución de la documentación para los objetivos de los sistemas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						gestión de la calidad
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
					2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.7.2 Tipos de documentos utilizados en los sistemas de gestión de Calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
					2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.
					2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	relación jurídica.				2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
					2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
					2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
					2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
					2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
					2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
					2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
					2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
					2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
					2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
					2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de	Distinción entre los requisitos para los sistemas de gestión de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Gestión de Calidad y requisitos para los productos.	calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	2.9 Mejora continua.	Acciones encaminadas a la mejora continua del sistema de gestión de la calidad.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
					2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
					2.8.3 Revisión del sistema de gestión de la calidad.	Evaluaciones sistemáticas para determinar la eficiencia y eficacia del sistema de gestión de la calidad.
					2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	2.6 Papel de la alta dirección dentro del sistema de gestión de la calidad.	Responsabilidades de la alta dirección para el establecimiento y operación del sistema de gestión de la calidad.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					sistemas de gestión de la calidad.	gestión de la calidad y de la organización.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos		Art. 62	Paso 8. Revisiones y Auditoría.	2.8 Evaluación de los sistemas de gestión de la calidad.	Procesos de evaluación y auditoría de los sistemas de gestión de la calidad.
					2.8.1 Procesos de evaluación dentro del sistema de gestión de la calidad.	Consideraciones para la evaluación del sistema de gestión de la calidad.
					2.8.2 Auditorías del sistema de gestión de la calidad.	Tipos de auditoría para determinar si se han alcanzado los requisitos del sistema de gestión de la calidad.
					2.8.3 Revisión del sistema de gestión de	Evaluaciones sistemáticas para determinar la eficiencia y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.				la calidad.	eficacia del sistema de gestión de la calidad.
					2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
					2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
					2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	2.5 Política de la Calidad y objetivos de la Calidad.	Documentos para proporcionar un punto de referencia para dirigir la organización.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	2.8.4 Autoevaluación.	Importancia de la autoevaluación para lograr la revisión completa y sistemática de las actividades y resultados de la organización.
					2.9 Mejora continua.	Acciones encaminadas a la mejora continua del sistema de gestión de la calidad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50	1. Recomendación General.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	contenido.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.					
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.
					2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.1 Base racional para los sistemas de gestión de Calidad.	Consideraciones para que los sistemas de gestión de la calidad ayuden a las organizaciones a aumentar la satisfacción de sus clientes.
					2.2 Requisitos para los sistemas de Gestión de Calidad y requisitos para los productos.	Distinción entre los requisitos para los sistemas de gestión de calidad y requisitos para los productos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.				2.3 Enfoque de sistemas de gestión de Calidad.	Etapas para contar con un enfoque para desarrollar e implementar un sistema de gestión de la calidad.
					2.4 Enfoque basado en procesos.	Adopción del enfoque basado en procesos para gestionar una organización.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones		Art. 70	1. Recomendación General	0.1 Generalidades.	Contexto de las normas ISO 9000 en la eficacia de los sistemas de gestión de la calidad.
					0.2 Principios de gestión de la Calidad.	Describe los principios de gestión de la calidad para la mejora del desempeño de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.				1 Objeto y campo de aplicación.	Aplicabilidad de los sistemas de gestión de la calidad.
					2 Fundamentos de los Sistemas de Gestión de Calidad.	Fundamentos de los sistemas de gestión de la calidad para la satisfacción de los clientes.
					3 Términos y definiciones.	Conceptos base para el manejo de sistemas de gestión de la calidad.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.7 Documentación.	Aspectos de la documentación en los sistemas de gestión de la calidad.
					2.7.1 Valor de la documentación.	Contribución de la documentación para los objetivos de los sistemas de gestión de la calidad.
					2.7.2 Tipos de documentos utilizados en los sistemas de gestión de la calidad.	Tipo de documentación a ser generada de acuerdo con los objetivos de los sistemas de gestión de la calidad y de la organización.

4.13 BS 10012:2009 Data Protection – Specification for a Personal Information Management System (PIMS).

Introducción. Introducción. Este estándar británico ha sido producido para formar las bases para las políticas internas sobre la legislación de protección de datos y el cumplimiento con las buenas prácticas. Asimismo, es un marco de referencia estándar para auditorías y procesos de revisión respecto a protección de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
					4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
					5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
					6 Mejora de un Sistema de Gestión de Información	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Personal.	relevantes.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	4.7 Procesamiento justo y lícito.	Actividades para que el procesamiento de información recopilada sea de forma licita y justa.
					4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.7.5 Terceros.	Actividades para la incorporación de procedimientos sobre el trato de información personal con terceros.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
					4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						relacionados.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.7.2 Registro de enunciados y avisos de privacidad.	Procedimientos para el mantenimiento de registros de enunciados o avisos de privacidad.
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	4.7.1 Recolección y procesamiento de información personal.	Procedimientos para asegurar el cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.7.3 Emisión de enunciados y avisos de privacidad.	Actividades para la emisión y presentación de aviso de privacidad.
					4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cumplimiento Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	4.7.5 Terceros.	Actividades para la incorporación de procedimientos sobre el trato de información personal con terceros.
					4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.
					4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.7.2 Registro de enunciados y avisos de privacidad.	Procedimientos para el mantenimiento de registros de enunciados o avisos de privacidad.
					4.7.4 Accesibilidad de enunciados y avisos de privacidad.	Procedimientos para la accesibilidad de avisos de privacidad y enunciados relacionados.
CALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	4.9.1 Idoneidad.	Procedimientos para asegurar que los datos recopilados son idóneos de acuerdo a los propósitos establecidos.
					4.9.2 Relevante y no excesivo.	Procedimientos para la recopilación de los datos mínimos necesarios.
					4.10 Precisión.	Actividades para el mantenimiento íntegro y actualizado de los datos recopilados.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.11 Retención y eliminación.	Actividades para asegurar que la información no es retenida más de lo necesario y que se elimina por medios apropiados.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	4.8 Procesamiento de información personal para propósitos especificados.	Actividades para asegurar que la información obtenida es utilizada solo para los propósitos especificados.
					4.8.1 Motivos para el tratamiento.	Actividades para asegurar que el tratamiento de datos se realizará de acuerdo a los propósitos especificados y bajo el marco legal pertinente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	4.9 Idoneidad, relevante y no excesivo.	Actividades para asegurar que la información personal es adecuada, relevante y no excesiva.
					4.9.1 Idoneidad.	Procedimientos para asegurar que los datos recopilados son idóneos de acuerdo a los propósitos establecidos.
					4.9.2 Relevante y no excesivo.	Procedimientos para la recopilación de los datos mínimos necesarios.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						vigentes.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	3 Planeación de un Sistema de Gestión de Información Personal.	Actividades de la etapa de planeación que dan soporte y dirección al PIMS.
					4 Implementación y operación de un Sistema de Gestión de Información Personal.	Actividades relacionadas a la asignación de roles y responsabilidades de acuerdo a la política privacidad que da soporte y dirección al PIMS.
					5 Monitoreo y revisión de un Sistema de Gestión de Información Personal.	Actividades para validar que se estén cumpliendo las políticas y procedimientos definidos en el PIMS.
					6 Mejora de un Sistema de Gestión de Información Personal.	Proceso de mejora continua del PIMS de acuerdo a los resultados del monitoreo y cambios relevantes.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
					4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						relacionados a la información personal.
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	3.3 Política de gestión de información personal.	La dirección de la organización debe mantener y demostrar compromiso con una política de gestión de información personal.
					3.4 Contenido de la política.	Lineamientos sobre el contenido de la política.
					3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	4.3 Entrenamiento y concientización.	Actividades para asegurar que el personal conozca sus responsabilidades cuando procesa información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS.
					5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	3.6 Provisión de recursos.	La organización determina y provee los recursos necesarios para el mantenimiento del PIMS.
					3.7 Incrustación del Sistema de Gestión de Información Personal en la cultura de la organización.	Actividades para incluir el PIMS como un valor relevante dentro de la organización

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS
					5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
					6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
					6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.12.2 Quejas y reclamaciones.	Procedimiento para la atención de quejas y reclamaciones.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.13 Cuestiones de Seguridad.	Actividades para asegurar que la información personal
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
					4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
					4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
					4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
					4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Medidas de Seguridad.	4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.13 Cuestiones de Seguridad.	Actividades para asegurar que la información personal
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
					4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
					4.13.3 Transmisión.	Procedimientos para la transmisión segura de información personal.
					4.13.4 Controles de acceso.	Establecer procedimientos para restringir el acceso a información personal solo a personal autorizado.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
					4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	3.4 Contenido de la política.	Lineamientos sobre el contenido de la política.
					4.2.1 General.	Debe ser mantenido un inventario de las categorías de información personal

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	3.5 Responsabilidad y rendición de cuentas.	Definición de la responsabilidad de sobre la información personal de acuerdo a la legislación vigente.
					4.1.1 Alta Dirección.	Un representante de la alta dirección designado como responsable de la información personal.
					4.1.2 Responsabilidad diaria para el cumplimiento con la política.	Designación de personal clave para vigilar el cumplimiento de políticas y procedimientos de información personal.
					4.1.3 Representantes de protección de datos.	Definición de responsables del procesamiento de información personal dentro de la organización.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.2.2 Información personal de riesgo alto.	Identificación y registro de información personal de alto riesgo.
					4.4 Evaluación de Riesgos.	Procedimiento para la administración de riesgos relacionados a la información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la mejora continua.
					6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
					6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	4.3 Entrenamiento y concientización.	Actividades para asegurar que el personal conozca sus responsabilidades cuando procesa información personal.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	4.13.2 Manejo y almacenamiento.	Procedimientos para el manejo y almacenamiento seguro de la información personal.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	4.13.1 Controles de Seguridad.	Establecimiento de controles con base en una evaluación de riesgos.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el		Art. 62	Paso 8. Revisiones y Auditoría.	4.5 Manteniendo actualizado el Sistema de Gestión de Información Personal.	Proceso para determinar que el PIMS se encuentra actualizado y conforme a los requerimientos de la regulación vigente.
					4.13.5 Revisiones de Seguridad.	Ejecución periódica de evaluaciones a los controles de seguridad.
					5.1 Auditoría interna.	Actividades para la ejecución de auditorías sobre el PIMS.
					5.2 Revisión gerencial.	Proceso de revisión del PIMS por parte de la gerencia orientado a la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					mejora continua.
					6.1 Acciones preventivas y correctivas.	Definición y seguimiento de acciones orientadas a la mejora del PIMS.
					6.2 Mejora continua.	Mejora de la eficacia del PIMS con respecto a las métricas establecidas.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	4.13.6 Gestión de incidentes de Seguridad.	Procedimientos para la identificación y tratamiento de incidentes de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50	1. Recomendación General.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que		Art. 51	Paso 7. Implementación de las Medidas de Seguridad	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	permita acreditar su existencia, alcance y contenido.			Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
51	Para el tratamiento de datos personales en		Art. 52 - II	Paso 7.	4.7.1 Recolección y	Procedimientos para asegurar el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de			Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	procesamiento de información personal.	cumplimiento con las leyes y regulaciones en cuanto a recopilación y procesamiento de información personal.
					4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
				TRANSFERENCIAS		
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.2 Consentimiento para nuevos propósitos.	Actividades para asegurar que el consentimiento de nuevos propósitos es otorgado e informado.
					4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	obligaciones que correspondan al responsable que transfirió los datos.				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo		Art. 70	1. Recomendación General	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.				4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4.8.3 Intercambios de datos.	Procedimientos donde se establezcan las responsabilidades de las partes para la transmisión de datos.
					4.16 Procesamiento subcontratado.	Procedimientos para asegurar que la información personal procesada por otra organización cumpla con los requerimientos y legislación vigentes.

4.14 NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.

Introducción. Este estándar proporciona principios y prácticas generalmente aceptadas para el aseguramiento de tecnologías de información. Los principios direccionan la seguridad desde un punto de vista de alto nivel; siendo las prácticas las que muestran lo que se debe hacer para mejorar y medir un programa de seguridad existente o en desarrollo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	2 Principios Generalmente Aceptados de Seguridad del Sistema.	Principios de seguridad utilizados como guía para el mantenimiento y desarrollo de programas de seguridad, políticas y procedimientos.
					3 Prácticas Comunes de Seguridad de TI.	Actividades mínimas a realizar para el establecimiento de un programa de seguridad.
LICITUD Y LEALTAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
					3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	3.4.6 Fase de Eliminación.	Actividades a considerar para el establecimiento de un proceso de eliminación seguro.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	2 Principios Generalmente Aceptados de Seguridad del Sistema.	Principios de seguridad utilizados como guía para el mantenimiento y desarrollo de programas de seguridad, políticas y procedimientos.
					3 Prácticas Comunes de Seguridad de TI	Actividades mínimas a realizar para el establecimiento de un programa de seguridad.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	3.1 Política.	Lineamientos para el establecimiento de una política de seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	3.8 Concientización y entrenamiento.	Establecimiento de un programa de concienciación y entrenamiento.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	2.7 La Seguridad en Cómputo debe ser reevaluada periódicamente.	Actividades para el monitoreo continuo y aceptación de la seguridad.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	2.3 La Seguridad en Cómputo debe ser costeable y efectiva.	Principio que indica que los costos de la seguridad no deben exceder los beneficios esperados.
					3.2 Gestión del Programa.	Actividades para la asignación de recursos y asignación de responsabilidades para el programa de seguridad.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	2.7 La Seguridad en Cómputo debe ser reevaluada periódicamente.	Actividades para el monitoreo continuo y aceptación de la seguridad.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	3.1 Política.	Lineamientos para el establecimiento de una política de seguridad.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.
					3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
					3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						rastreabilidad y responsabilidad en la identificación y autenticación.
					3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
					3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
					3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.13.1 Contenidos de los registros de auditoría.	Establece las características básicas del contenido de auditoría.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.
					3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
					3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						la identificación y autenticación.
					3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
					3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
					3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	3.6.2 Identificar recursos.	Actividades para la identificación de recursos con funciones críticas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
					3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	2.7 La Seguridad en Cómputo debe ser reevaluada periódicamente.	Actividades para el monitoreo continuo y aceptación de la seguridad.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	3.8 Concientización y entrenamiento.	Establecimiento de un programa de concienciación y entrenamiento.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	3.6.2 Identificar recursos.	Actividades para la identificación de recursos con funciones críticas.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales	3.3.2 Mitigación del Riesgo.	Actividades para la selección e implementación de controles para la reducción del riesgo identificado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				documentadas.	3.6.2 Identificar recursos.	Actividades para la identificación de recursos con funciones críticas.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	3.3.1 Evaluación del Riesgo.	Actividades para la identificación, análisis e interpretación de riesgos.
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3.7 Manejo de Incidentes de Seguridad en Cómputo.	Proceso para el tratamiento de incidentes de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que		Art. 50	1. Recomendación General.	2.8 La Seguridad en Cómputo está limitada por factores sociales.	Limitaciones al programa de seguridad por implicaciones externas a la organización y prácticas aceptadas.
					3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.
					3.10 Seguridad física y ambiental	Actividades para la implementación de seguridad física y control ambiental.
					3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
					3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
					3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	2.8 La Seguridad en Cómputo está limitada por factores sociales.	Limitaciones al programa de seguridad por implicaciones externas a la organización y prácticas aceptadas.
					3.9 Consideraciones de Seguridad en el Soporte y Operaciones de	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Medidas de Seguridad.	Cómputo.	
					3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
					3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
					3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
					3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
					3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	2.8 La Seguridad en Cómputo está limitada por factores sociales.	Limitaciones al programa de seguridad por implicaciones externas a la organización y prácticas aceptadas.
					3.9 Consideraciones de Seguridad en el Soporte y Operaciones de Cómputo.	Actividades a implementar relacionadas al soporte de las operaciones para prevenir fallas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Seguridad.	3.10 Seguridad física y ambiental.	Actividades para la implementación de seguridad física y control ambiental.
					3.11 Identificación y autenticación.	Prácticas para la definición de controles para mantener la rastreabilidad y responsabilidad en la identificación y autenticación.
					3.12 Control de acceso lógico.	Actividades para restringir el acceso al personal de acuerdo a sus responsabilidades o tareas.
					3.13 Registros de auditoría.	Establece que se debe de mantener un record de registros de actividad y accesos.
					3.14 Criptografía.	Establece controles para el uso apropiado de las herramientas criptográficas en el tratamiento de información.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.5 Las responsabilidades y la rendición de cuentas de la Seguridad en Cómputo deben ser hechas explícitas.	Establecimiento de las responsabilidades a cada uno de los actores involucrados en el programa.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	3.4 Planeación del Ciclo de Vida.	Define las actividades para la administración del ciclo de vida del programa de seguridad.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

4.15 OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.

Introducción. Estos lineamientos establecen un marco de trabajo de los principios que aplican a todos los participantes de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la mejora de la seguridad de los sistemas de información y las redes a fin de promover la prosperidad económica y el desarrollo social.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
					2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
					3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
					4. Ética.	Los participantes deben respetar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						los intereses legítimos de otros.
					5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
					6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
					7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
					8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
					9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
LICITUD Y LEALTAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						democrática.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Medidas de Seguridad.		
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la		Art. 48 - I	Paso 2. Política de Gestión de Datos	2. Responsabilidad.	Todos los participantes son responsables de la seguridad de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	organización.			Personales.		los sistemas de información y las redes.
					8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de negocios, así como para mitigarlos.					
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	9. Reevaluación.	Los participantes deben revisar y reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que ellos pueden hacer para mejorar la seguridad.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.		Art. 50	1. Recomendación General.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
					8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5. Democracia	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Cumplimiento Cotidiano de Medidas de Seguridad.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Cumplimiento Cotidiano de Medidas de Seguridad.	8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una		Art. 70	1. Recomendación General	1. Concientización.	Los participantes deben estar conscientes de la necesidad por la seguridad de los sistemas de información y las redes y lo que

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.					ellos pueden hacer para mejorar la seguridad.
					2. Responsabilidad.	Todos los participantes son responsables de la seguridad de los sistemas de información y las redes.
					3. Respuesta.	Los participantes deben actuar en una manera oportuna y cooperativa para prevenir, detectar, y responder a los incidentes de seguridad.
					4. Ética.	Los participantes deben respetar los intereses legítimos de otros.
					5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.
					6. Evaluación del riesgo.	Los participantes deben ejecutar evaluaciones del riesgo.
					7. Diseño e implementación de la seguridad.	Los participantes deben incorporar la seguridad con un elemento esencial de los sistemas de información y las redes.
					8. Gestión de la seguridad.	Los participantes deben adoptar un enfoque exhaustivo para la gestión de la seguridad.
					9. Reevaluación.	Los participantes deben revisar y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						reevaluar la seguridad de los sistemas de información y las redes, y hacer modificaciones apropiadas a las políticas, prácticas, medidas, y procedimientos de seguridad.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5. Democracia.	La seguridad de los sistemas de información y las redes deben ser compatibles con los valores esenciales de una sociedad democrática.

4.16 Generally Accepted Privacy Principles (GAPP) from American Institute of CPAs.

Introducción. Este documento desarrollado desde una perspectiva de negocio. El documento está desarrollado con base en 10 principios de privacidad, tomando como referencia la mayoría de las regulaciones locales, nacionales e internacionales. Cada uno de los principios es soportado por un objetivo medible.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	1 Gestión.	Actividades para la definición de documentación, comunicados y asignación de responsabilidades de acuerdo a las políticas y procedimientos.
					2 Aviso.	Proveer aviso sobre políticas y procedimientos de privacidad e identificar los propósitos de la recopilación de información personal.
					3 Opción y Consentimiento.	Describir las opciones sobre el consentimiento respecto a la recopilación de información personal.
					4 Recolección.	Recopilar información solo para los propósitos definidos.
					5 Uso, retención, y eliminación.	Establecimiento de los lineamientos para limitar el uso,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						retención y eliminación de información personal.
					6 Acceso.	Proveer al titular acceso para la revisión y actualización de sus datos.
					7 Divulgación a terceros.	Delimita la transmisión de información a terceros solo para los propósitos establecidos.
					8 Seguridad para Privacidad.	Actividades para la protección de datos personales contra accesos no autorizados.
					9 Calidad.	La entidad mantiene la información completa, actualizada y actual.
					10 Monitoreo y cumplimiento.	Actividades para asegurar el cumplimiento de las políticas de privacidad.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	4.1.0 Política de Privacidad.	Alineación de políticas de privacidad a la colección de información personal.
					4.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					4.1.2 Tipos de información personal recopilada y métodos de recopilación.	Métodos para la recolección de información y tipos de información de acuerdo al aviso de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
					4.2.2 Recolección por medios justos y legales.	Métodos para la recolección de información revisados por la dirección.
					4.2.3 Recolección mediante terceros.	La dirección confirma que los terceros de donde recopila información son seguros y legales.
					4.2.4 Información desarrollada sobre individuos.	Procedimientos por el cual se informa al titular si se adquiere información personal.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	3.1.0 Política de Privacidad.	Definición de la política de privacidad.
					3.1.1 Comunicación a individuos.	Comunicación al titular sobre las opciones para la recopilación de información.
					3.1.2 Consecuencias de negar o retirar el consentimiento.	Informar al titular sobre las consecuencias de negar a proporcionar información personal, negar o retirar el consentimiento.
					3.2.1 Consentimiento implícito o explícito.	Obtención del consentimiento en el momento o antes de la recopilación de datos personales.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos	3.1.0 Política de Privacidad.	Definición de la política de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	su consentimiento expreso.			Personales.	3.1.1 Comunicación a individuos.	Comunicación al titular sobre las opciones para la recopilación de información.
					3.1.2 Consecuencias de negar o retirar el consentimiento.	Informar al titular sobre las consecuencias de negar a proporcionar información personal, negar o retirar el consentimiento.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	3.2.3 Consentimiento explícito para información sensible.	Obtención de consentimiento explícito siempre que se recopile información sensible.
					4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
					5.2.1 Uso de información personal.	Indica que la información personal es utilizada solo para los propósitos establecidos después de la obtención del consentimiento del titular.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	3.1.0 Política de Privacidad.	Definición de la política de privacidad.
					3.1.1 Comunicación a individuos.	Comunicación al titular sobre las opciones para la recopilación de información.
					3.2.1 Consentimiento implícito o explícito.	Obtención del consentimiento en el momento o antes de la recopilación de datos personales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Medidas de Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
					2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
					2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuáles son los procesos y actividades cubiertas por dichas políticas y procedimientos.
					4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
					2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
					2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
					4.2.3 Recolección mediante terceros.	La dirección confirma que los terceros de donde recopila información son seguros y legales.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
CALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
					9.2.1 Exactitud de información personal.	La información recopilada debe ser exacta y completa.
					9.2.2 Relevancia de información personal.	La información personal debe ser relevante a los propósitos establecidos
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	5.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					5.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
					5.2.1 Uso de información personal.	La información personal recopilada solo puede ser utilizada para los propósitos definidos.
					5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
					5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	5.2.1 Uso de información personal.	La información personal recopilada solo puede ser utilizada para los propósitos definidos.
					5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
					5.2.3 Disposición,	Procedimientos para la eliminación

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					destrucción, borrado de información personal.	segura de información personal.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
					5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
					2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
					2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuáles son los procesos y actividades cubiertas por dichas políticas y procedimientos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
					2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
					2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuáles son los procesos y actividades cubiertas por dichas políticas y procedimientos.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuáles son los procesos y actividades cubiertas por dichas políticas y procedimientos.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
					8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en		Art. 48 - II	Paso 9. Mejora Continua y Capacitación.	1.1.1 Comunicación a personal interno.	Políticas, procedimientos Sanciones relacionadas a privacidad deben ser comunicadas

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	materia de protección de datos personales.			Capacitación.		al personal interno.
					1.1.2 Responsabilidad y rendición de cuentas de las Políticas.	Asignación de roles y responsabilidades sobre privacidad deben ser establecidas y comunicadas.
					1.2.9 Calificaciones de personal interno.	Características apropiadas del personal responsable de privacidad.
					1.2.10 Entrenamiento y concientización de privacidad.	Se debe proporcionar entrenamiento sobre privacidad al personal con funciones relacionadas relevantes.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
					1.2.2 Consistencia de políticas y procedimientos con leyes y regulaciones.	Políticas y procedimientos revisados para que sean consistentes con leyes y regulaciones vigentes.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de seguridad.
					1.2.8 Recursos de soporte.	Recursos suficientes para la implementación de las políticas de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
					1.2.6 Gestión de infraestructura y sistemas.	Procesos para la administración y control de la infraestructura que soporta el almacenamiento y procesamiento de información personal.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
					1.2.2 Consistencia de políticas y procedimientos con leyes y regulaciones.	Políticas y procedimientos revisados para que sean consistentes con leyes y regulaciones vigentes.
					1.2.11 Cambios en requerimientos regulatorios y de negocio.	Procedimiento para el monitoreo de cambios en leyes y regulaciones.
					8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de	10.2.1 Proceso de atención de dudas, quejas y disputas.	Procedimiento para la atención de quejas y disputas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	10.2.2 Resolución de disputas.	Base de conocimiento sobre la resolución de quejas y disputas.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	1.1.1 Comunicación a personal interno.	Políticas, procedimientos Sanciones relacionadas a privacidad deben ser comunicadas al personal interno.
					1.1.2 Responsabilidad y rendición de cuentas de las Políticas.	Asignación de roles y responsabilidades sobre privacidad deben ser establecidas y comunicadas.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
					8.2.2 Controles de Acceso Lógico.	Procedimientos para la restricción de acceso lógico a información personal.
					8.2.3 Controles de Acceso Físico.	Procedimientos para la restricción de acceso físico a información personal.
					8.2.4 Salvaguardas Ambientales.	Establecimiento de controles ambientales para la protección de información personal.
					8.2.5 Información	Controles para la transmisión

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					personal transmitida.	segura de datos personales.
					8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
					8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.2.2 Controles de Acceso Lógico.	Procedimientos para la restricción de acceso lógico a información personal.
					8.2.3 Controles de Acceso Físico.	Procedimientos para la restricción de acceso físico a información personal.
					8.2.5 Información personal transmitida.	Controles para la transmisión segura de datos personales.
					8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	6.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					6.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
					8.2.2 Controles de Acceso Lógico.	Procedimientos para la restricción de acceso lógico a información personal.
					8.2.3 Controles de Acceso Físico.	Procedimientos para la restricción de acceso físico a información personal.
					8.2.4 Salvaguardas Ambientales.	Establecimiento de controles ambientales para la protección de información personal.
					8.2.5 Información personal transmitida.	Controles para la transmisión segura de datos personales.
					8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
					8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente,	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos	1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.			Personales.	1.2.11 Cambios en requerimientos regulatorios y de negocio.	Procedimiento para el monitoreo de cambios en leyes y regulaciones.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	1.2.3 Identificación y clasificación de información personal.	Inventario de información personal y datos sensibles.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	1.2.9 Calificaciones de personal interno.	Características apropiadas del personal responsable de privacidad.
					1.2.10 Entrenamiento y concientización de privacidad.	Se debe proporcionar entrenamiento sobre privacidad al personal con funciones

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						relacionadas relevantes.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
					8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
					8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
					8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
					8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	8.2.1 Programa de Seguridad de la Información.	Documentación y formalización de un programa de seguridad de la información.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	8.2.7 Pruebas de Salvaguardas de Seguridad.	Procedimientos de prueba para la eficacia de los controles establecidos.
					10.2.3 Revisión de cumplimiento.	El cumplimiento con las leyes y regulaciones vigentes, contratos y
					10.2.4 Instancias de no cumplimiento.	El incumplimiento con leyes regulaciones o contratos deben ser documentadas y corregidas.
					10.2.5 Monitoreo continuo.	Procedimientos para el monitoreo periódico de la efectividad del sistema
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	1.2.9 Calificaciones de personal interno.	Características apropiadas del personal responsable de privacidad.
					1.2.10 Entrenamiento y concientización de privacidad.	Se debe proporcionar entrenamiento sobre privacidad al personal con funciones

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						relacionadas relevantes.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	8.2.6 Información personal en medios móviles.	Controles para la restricción de acceso a la información personal en medios móviles.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	8.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					8.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					8.2.1 Programa de Seguridad de la Información.	8.2.1 Programa de Seguridad de la Información.
					8.2.2 Controles de Acceso Lógico.	8.2.2 Controles de Acceso Lógico.
					8.2.3 Controles de Acceso Físico.	8.2.3 Controles de Acceso Físico.
					8.2.4 Salvaguardas Ambientales.	8.2.4 Salvaguardas Ambientales.
					8.2.5 Información personal transmitida.	8.2.5 Información personal transmitida.
					8.2.6 Información personal en medios móviles.	8.2.6 Información personal en medios móviles.
43	Actualizar las medidas de seguridad cuando:		Art. 62	Paso 8. Revisiones y Auditoría.	1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.				1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración de manera periódica.
					1.2.2 Consistencia de políticas y procedimientos con leyes y regulaciones.	Políticas y procedimientos revisados para que sean consistentes con leyes y regulaciones vigentes.
					1.2.4 Evaluación de riesgo.	Metodología para la evaluación de riesgos relacionados a información personal.
					1.2.6 Gestión de infraestructura y sistemas.	Procesos para la administración y control de la infraestructura que soporta el almacenamiento y procesamiento de información personal.
					1.2.11 Cambios en requerimientos regulatorios y de negocio.	Procedimiento para el monitoreo de cambios en leyes y regulaciones.
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	1.2.7 Gestión de incidentes y brechas de privacidad.	Proceso formal para la gestión de brechas e incidentes de privacidad.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	1.2.7 Gestión de incidentes y brechas de privacidad.	Proceso formal para la gestión de brechas e incidentes de privacidad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	1.2.7 Gestión de incidentes y brechas de privacidad.	Proceso formal para la gestión de brechas e incidentes de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	efecto de evitar que la vulneración se repita.					
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos		Art. 50	1. Recomendación General.	1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
					5.2.3 Disposición, destrucción, borrado de información personal.	Procedimientos para la eliminación segura de información personal.
					7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
					7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.			Cotidiano de Medidas de Seguridad.	7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de seguridad.
					1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Cotidiano de Medidas de Seguridad.	7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	1.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de seguridad.
					1.2.1 Revisión y aprobación.	Las políticas y procedimientos de privacidad deben ser revisados y aprobados por la administración

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		de manera periódica.
					1.2.5 Consistencia de compromisos con políticas y procedimientos de privacidad.	Los contratos deben ser concisos con las políticas y procedimientos de privacidad.
					4.2.1 Recolección limitada a propósitos identificados.	La información recopilada es solo para los propósitos especificados en el aviso.
					5.2.2 Retención de información personal.	Actividades para no retener información más de lo necesario.
					7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos	Se puede divulgar información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					propósitos y usos.	para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.1.0 Política de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					2.1.1 Comunicación a individuos.	Comunicación al titular sobre el uso, retención y eliminación de su información personal.
					2.2.1 Provisión de aviso.	Se comunica al titular sobre las políticas y procedimientos de privacidad antes de la recopilación de datos.
					2.2.2 Entidades y actividades cubiertas.	Dentro del aviso se incluye cuáles son los procesos y actividades cubiertas por dichas políticas y procedimientos.
					2.2.3 Claro y conciso.	El aviso de privacidad debe ser visible y con lenguaje claro.
					7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de	Información personal divulgada

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información personal.	solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	7.1.0 Políticas de Privacidad.	Criterios para el establecimiento de la política de privacidad.
					7.1.1 Comunicación a individuos.	Comunicación a los titulares sobre los propósitos de la colección de información.
					7.1.2 Comunicación a terceros.	Comunicación sobre políticas de privacidad a terceros que les sea compartida información.
					7.2.1 Divulgación de información personal.	La divulgación de información personal a terceros debe ser con base en los propósitos establecidos.
					7.2.2 Protección de información personal.	Información personal divulgada solo si hay acuerdos y conforme a las políticas de privacidad establecidas.
					7.2.3 Nuevos propósitos y usos.	Se puede divulgar información para nuevos propósitos solo si se tiene el consentimiento del titular.
					7.2.4 Mal uso de información personal por terceros.	Actividades de remediación en caso de mal uso de información por parte de un tercero.

4.17 Control Objectives for Information and Related Technology (COBIT v4.1).

Introducción. COBIT 4.1 es un marco de referencia para la implementación del gobierno y gestión de los recursos de TI en las organizaciones. Su objetivo es proporcionar valor a la organización por medio de un coste óptimo de recursos, a la vez que los riesgos son controlados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	PO2 Definir la Arquitectura de la Información.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
					PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					AI6 Administrar cambios.	Definición de políticas y procedimientos para la administración de cambios.
					AI7 Instalar y acreditar soluciones y cambios.	Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación
					DS4 Garantizar la continuidad del	Definición de políticas y procedimientos de gestión de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					servicio.	continuidad así como planes de contingencia
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
					DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio
					DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	hacerse a través de medios engañosos o fraudulentos.					
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	PO2.1 Modelo de Arquitectura de Información Empresarial.	Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI.
					PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos.	Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización.
					PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						y sensible es la información de la empresa.
					PO2.4 Administración de Integridad.	Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico.
					PO8.3 Estándares de Desarrollo y de Adquisición.	Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados.
					DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
					DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
					DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
					DS11.2 Acuerdos de	Definir e implementar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Almacenamiento y Conservación.	procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
					DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.
					DS11.5 Respaldo y Restauración.	Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de los datos.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
					DS11.2 Acuerdos de Almacenamiento y Conservación.	Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente.
					DS11.4 Eliminación.	Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.
					DS11.5 Respaldo y Restauración.	Definir e implementar procedimientos de respaldo y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.				DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	DS11.1 Requerimientos del Negocio para Administración de Datos.	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos	PO4.14 Políticas y Procedimientos para	Asegurar que los consultores y el personal contratado que soporta

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.			Personales.	Personal Contratado.	la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
					PO4.15 Relaciones.	Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI.
					DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	PO2 Definir la Arquitectura de la Información.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					AI6 Administrar cambios.	Definición de políticas y procedimientos para la administración de cambios.
					AI7 Instalar y acreditar soluciones y cambios.	Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación.
					DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
					DS4 Garantizar la continuidad del servicio.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia.
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11 Administrar los	Optimizar el uso de la información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					datos.	y garantizar la disponibilidad de la información cuando se requiera.
					DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
					DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	PO8 Administrar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales
					AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
					DS5 Garantizar la	Establecer políticas y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de los sistemas.	procedimientos para la gestión de la seguridad de la información.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
					DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	PO6.1 Ambiente de Políticas y de Control.	Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.
					PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI.	Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y el control que se alinee con la política de TI, el ambiente de control y el marco de trabajo de riesgo y control de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						empresa.
					DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	PO7.4 Entrenamiento del Personal de TI.	Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar y mejorar su conocimiento.
					DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
					DS7 Educar y Entrenar a los Usuarios.	Educar y entrenar a los usuarios respecto a los servicios de TI ofrecidos.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías		Art. 48 - III	Paso 8. Revisiones y Auditoría.	PO8.6 Medición, Monitoreo y Revisión	Definir, planear e implementar mediciones para monitorear el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	externas para comprobar el cumplimiento de las políticas de privacidad.				de la Calidad.	cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
					DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
					ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	DS5.1 Administración de la Seguridad de TI.	Administrar la seguridad de TI al nivel más alto apropiado en la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
					DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
24	Instrumentar un procedimiento para que se		Art. 48 - V	Paso 5. Realizar el	PO9 Evaluar y	La elaboración de un marco de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.			Análisis de Riesgo de los Datos Personales.	Administrar los Riesgos de TI.	trabajo de administración de riesgos el cual está integrado en los marcos gerenciales.
					AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
					DS5.1 Administración de la Seguridad de TI.	Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
					DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
					DS5.11 Intercambio de Datos Sensitivos.	Transacciones de datos sensibles se intercambian solo a través de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
					ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
					DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
					ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DS8.1 Mesa de Servicios.	Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.
					DS8.2 Registro de Consultas de Clientes.	Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.
					DS8.3 Escalamiento	Establecer procedimientos de mesa de servicios de manera que

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de Incidentes.	los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas.
					DS8.4 Cierre de Incidentes.	Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
					DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
					DS5.6 Definición de Incidente de	Definir claramente y comunicar las características de incidentes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Seguridad.	seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
					PO3.4 Estándares Tecnológicos.	Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas.
					PO4.9 Propiedad de los datos y sistemas.	Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información.
					AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						con la clasificación de datos
					AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
					DS12.3 Acceso Físico.	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias.
					DS11.6 Requerimientos de	Definir e implementar las políticas y procedimientos para identificar y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Seguridad para la Administración de Datos.	aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AI2.3 Control y Posibilidad de Auditar las Aplicaciones.	Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.
					DS5.3 Administración de Identidad.	Asegurar que todos los usuarios y su actividad en sistemas de TI deben ser identificables de manera única.
					DS5.11 Intercambio de Datos Sensitivos.	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.
					DS11.1 Requerimientos del Negocio para	Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Administración de Datos.	forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento.	Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado.
					DS5.1 Administración de la Seguridad de TI.	Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de	PO2.3 Esquema de Clasificación de	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.			seguridad y Análisis de Brecha.	Datos.	y sensible es la información de la empresa.
					AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
					DS12 Administrar el	Proteger los activos de cómputo y la información del negocio

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					ambiente físico.	minimizando el riesgo de una interrupción del servicio.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales.
					AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
					AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				DS5.2 Plan de Seguridad de TI.	Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	PO2.3 Esquema de Clasificación de Datos.	Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información de la empresa.
					DS9 Administrar la configuración.	Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.
					DS11.3 Sistema de	Definir e implementar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Administración de Librerías de Medios.	procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.
					DS13.4 Documentos Sensitivos y Dispositivos de Salida.	Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	PO4.9 Propiedad de los datos y sistemas.	Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales.
					AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						para el desarrollo de los requerimientos.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos.
					AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.
					DS5.3 Administración de Identidad.	Asegurar que todos los usuarios y su actividad en sistemas de TI deben ser identificables de manera única.
					DS5.4 Administración de Cuentas del Usuario.	Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados estén

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						controlados por medio de políticas y procedimientos.
					DS5.7 Protección de la Tecnología de Seguridad.	Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.
					DS5.8 Administración de Llaves Criptográficas.	Determinar las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas
					DS5.9 Prevención, Detección y Corrección de Software Malicioso.	Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware.
					DS5.10 Seguridad de la Red.	Uso de técnicas de seguridad y procedimientos de administración

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
					DS5.11 Intercambio de Datos Sensitivos.	Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
					ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
					ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
					DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
					ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						operativos identificados.
					ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	PO7.4 Entrenamiento del Personal de TI.	Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar y mejorar su conocimiento,
					DS7 Educar y Entrenar a los Usuarios.	Educar y entrenar a los usuarios respecto a los servicios de TI ofrecidos.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	DS9 Administrar la configuración.	Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DS11.3 Sistema de Administración de Librerías de Medios.	Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	AI2.4 Seguridad y Disponibilidad de las Aplicaciones.	Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos
					AI3.2 Protección y Disponibilidad del Recurso de Infraestructura.	Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	PO8.6 Medición, Monitoreo y Revisión de la Calidad.	Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona.
					PO9 Evaluar y Administrar los Riesgos de TI.	La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales
					AI1.2 Reporte de Análisis de Riesgos.	Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.
					AI3.3 Mantenimiento de la Infraestructura.	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						administración de cambios de la organización.
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
					DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
					DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.	Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.
					DS5.6 Definición de Incidente de Seguridad.	Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados y tratados apropiadamente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DS10.2 Rastreo y Resolución de Problemas.	El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y		Art. 50	1. Recomendación General.	PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
					PO4.15 Relaciones.	Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI.
					AI5.2 Administración de Contratos con Proveedores.	Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores.
					DS1 Definir y administrar los niveles	Identificación de requerimientos de servicio, el acuerdo de niveles

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				de servicio.	de servicio y el monitoreo del cumplimiento de los niveles de servicio.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
					DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.	PO7.6 Procedimientos de Investigación del Personal.	Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI.
					DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cumplimiento Cotidiano de Medidas de Seguridad.	DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
					AI5.2 Administración de Contratos con Proveedores.	Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores.
					DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio
					DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	PO4.14 Políticas y Procedimientos para Personal Contratado.	Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa.
					AI5.2 Administración de Contratos con Proveedores.	Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores.
					DS1 Definir y administrar los niveles de servicio.	Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.
					DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					de los beneficios, riesgos y costos.
					DS5 Garantizar la seguridad de los sistemas.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DS11 Administrar los datos.	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.
					DS12 Administrar el ambiente físico.	Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio.
					DS13 Administrar las operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.
					DS12.2 Medidas de Seguridad Física.	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.
					ME2 Monitorear y Evaluar el Control Interno.	Monitorear y evaluar el control interno en relación a los objetivos de negocio y a los riesgos operativos identificados.
					ME3 Garantizar el Cumplimiento Regulatorio.	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de	DS1 Definir y administrar los niveles de servicio.	Asegurar la alineación de los servicios claves de TI con la estrategia del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DS2 Administrar los servicios de terceros.	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.
					DS11.6 Requerimientos de Seguridad para la Administración de Datos.	Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos.

4.18 Control Objectives for Information and Related Technology (COBIT 5).

Introducción. COBIT 5 es un marco de referencia para la implementación del gobierno y gestión de los recursos de Tecnología de la Información en las organizaciones. Su objetivo es proporcionar valor a la organización por medio de un coste óptimo de recursos, a la vez que los riesgos son controlados. COBIT 5 toma en cuenta las versiones anteriores, y añade mejoras en procesos, prácticas, actividades, métricas, y modelos de madurez principalmente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	APO03 Administrar la Arquitectura Empresarial.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
					APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					BAI06 Gestionar los Cambios.	Definición de políticas y procedimientos para la administración de cambios.
					BAI07 Gestionar la Aceptación del Cambio y de la Transición.	Formalizar la implementación de cambio a través de procedimientos donde se incluya a los usuarios.
					DSS01 Gestionar las	Establecer políticas y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Operaciones.	procedimientos para la entrega de servicios de TI.
					DSS04 Gestionar la Continuidad.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los	Asegurar que los puestos de usuario final se encuentren

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					puestos de usuario final.	asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.					información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes,	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.					dominios negocio, información, datos, aplicaciones y tecnología.
					APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
					APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad.	Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC
					APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	Criterios para incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollo de soluciones y los servicios ofrecidos.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.					dominios negocio, información, datos, aplicaciones y tecnología.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
					DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
13	El responsable establecerá y documentará		Art. 38	Paso 2. Política de	APO03.02 Definir la	La arquitectura de referencia

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.			Gestión de Datos Personales.	arquitectura de referencia.	describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
					DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.	Actividades para asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan.
					DSS06.06 Asegurar los activos de	Asegurar el acceso a los activos de información por métodos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información.	apropiados.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					autorización.	
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS06.04 Gestionar errores y excepciones.	Criterios para la definición de un proceso para la gestión de errores y excepciones.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
					DSS06.05 Asegurar la trazabilidad de los	Actividades para asegurar que la información de negocio puede ser

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					eventos y responsabilidades de información.	rastreada hasta los responsables y eventos de negocio que la originan.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los	Criterios para que los usuarios tengan los derechos apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					activos de TI.	de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la	Criterios para que los usuarios

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					identidad del usuario y el acceso lógico.	tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO01.01 Definir la estructura organizativa.	Criterios para la definición de una estructura que cubra las necesidades de la organización.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	APO03 Administrar la Arquitectura Empresarial.	Conceptos para el establecimiento de una arquitectura que incluya los procesos de negocio y los diferentes componentes de TI.
					APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					BAI06 Gestionar los Cambios.	Definición de políticas y procedimientos para la administración de cambios.
					BAI07 Gestionar la Aceptación del Cambio y de la Transición.	Formalizar la implementación de cambio a través de procedimientos donde se incluya a los usuarios.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los	Criterios para la administración de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Proveedores.	proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS04 Gestionar la Continuidad.	Definición de políticas y procedimientos de gestión de la continuidad así como planes de contingencia
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	APO11 Gestionar la Calidad.	Definir y comunicar los requisitos de calidad en todos los procesos de la organización.
					APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	EDM03.02 Orientar la gestión de riesgos.	Orientar el establecimiento de prácticas de gestión de riesgos a asegurar que no se exceda el apetito del riesgo.
					APO01.03 Mantener los elementos catalizadores del sistema de gestión.	Actividades para el mantenimiento de elementos catalizadores dentro de los objetivos de la organización.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición de actividades de tratamiento de riesgos de seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	APO07.03 Mantener las habilidades y competencias del personal.	Actividades para el entrenamiento continuo del personal.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					APO07 Gestionar los Recursos Humanos.	Criterios para la gestión de RH respecto a sus habilidades, capacidades, y responsabilidades dentro de la organización.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
					DSS05.07 Supervisar la infraestructura para detectar eventos	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					relacionados con la seguridad.	accesos no autorizados y asegurar que cualquier evento esté contemplado.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los	Identificar, documentar, priorizar y mitigar los riesgos funcionales y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					requerimientos.	técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					final.	la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
					DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.	Procedimientos para el registro y gestión de incidentes.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS02.04 Investigar, diagnosticar y localizar incidentes.	Procedimientos para el diagnóstico, investigación y localización de incidentes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						seguridad.
					DSS02.05 Resolver y recuperarse de incidentes.	Procedimientos para la resolución y recuperación de servicios afectados por incidentes de seguridad.
					DSS02.06 Cerrar peticiones de servicio e incidentes.	Criterios para el cierre de incidentes y solicitudes de servicio.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición del plan de tratamiento de riesgos.
					DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					APO03.05 Proveer los servicios de arquitectura empresarial.	Guías de los proyectos, formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación de los valores aportados por la arquitectura.
					APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
					BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis	BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tratamiento.			de Brecha.	APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar	Criterios para el establecimiento

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					roles, responsabilidades, privilegios de acceso y niveles de autorización.	de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.				BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					DSS06 Gestionar los Controles de los	Criterios para la definición y mantenimiento de controles a lo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Procesos de la Empresa.	largo de los procesos de negocio.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
					BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
					APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Criterios para la definición de actividades de tratamiento de riesgos de seguridad.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					final.	la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	APO03.02 Definir la arquitectura de referencia.	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.
					BAI10 Gestionar la Configuración.	Definir y mantener registros y relaciones entre los principales

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						recursos y capacidades necesarios para la prestación de servicios.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
					DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	Criterios para la disponibilidad de información sensible y el acceso a medios de salida.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	APO01.06 Definir la propiedad de la información (datos) y del sistema.	Criterios para la definición de dueños de información y de los sistemas que la procesan.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						auditabilidad.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.01 Proteger contra software malicioso (malware).	Actividades de control contra software malicioso.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					APO13.01 Establecer y mantener un SGSI.	Criterios para el establecimiento y mantenimiento de un SGSI.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					APO13.03 Supervisar y revisar el SGSI.	Criterios para la supervisión y revisión del sistema de gestión por parte de la Dirección.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y	APO11.04 Supervisar	Actividades para planear y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Auditoría.	y hacer controles y revisiones de calidad.	monitorear los controles de calidad implementados.
					DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	APO07.03 Mantener las habilidades y competencias del personal.	Actividades para el entrenamiento continuo del personal.
					APO07 Gestionar los Recursos Humanos.	Criterios para la gestión de RH respecto a sus habilidades, capacidades, y responsabilidades

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						dentro de la organización.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	BAI10 Gestionar la Configuración	Definir y mantener registros y relaciones entre los principales recursos y capacidades necesarios para la prestación de servicios.
					DSS04.08 Ejecutar revisiones postreanudación.	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	BAI03.01 Diseñar soluciones de alto nivel.	Criterios para desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas.
					BAI03.02 Diseñar los componentes detallados de la solución.	Criterios para la elaboración de diseños progresivos considerando todos los componentes.
					BAI03.03 Desarrollar los componentes de la solución.	Criterios para desarrollar los componentes de la solución conforme el diseño siguiendo los métodos de desarrollo, estándares

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de documentación, requerimientos de calidad (QA) y estándares de aprobación.
					BAI03.05 Construir soluciones.	Criterios para la construcción de soluciones e integrarlas con los procesos de negocio, seguridad y auditabilidad.
					DSS02.03 Verificar, aprobar y resolver peticiones de servicio.	Actividades y métodos para aprobar y solucionar incidentes y peticiones de servicio.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario	Criterios para que los usuarios tengan los derechos apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					y el acceso lógico.	de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el		Art. 62	Paso 8. Revisiones y Auditoría.	APO11.04 Supervisar y hacer controles y revisiones de calidad.	Actividades para planear y monitorear los controles de calidad implementados.
					APO12 Gestionar el Riesgo.	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
					BAI02.03 Gestionar los riesgos de los requerimientos.	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					de la información y asociados con los requerimientos de la empresa.
					BAI03.10 Mantener soluciones.	Criterios para desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Actividades para la detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté contemplado.
					DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.	Criterios para la definición de la clasificación de incidentes y solicitudes de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS03.02 Investigar y diagnosticar problemas.	Criterios para el proceso de investigación y diagnóstico de problemas.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.		Art. 50	1. Recomendación General.	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO01.01 Definir la estructura organizativa.	Criterios para la definición de una estructura que cubra las necesidades de la organización.
					APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS05 Gestionar los	Establecer políticas y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.				Servicios de Seguridad.	procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	APO07.01 Mantener la dotación de personal suficiente y adecuado.	Criterios para mantener solo a personal necesario de acuerdo a las necesidades del negocio.
					APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de	APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.	Criterios para la identificación y categorización de proveedores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.			Medidas de Seguridad.	APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los	APO07.06 Gestionar el personal contratado.	Monitorear que el personal contratado tiene las capacidades necesarias y cumple con las políticas de la organización.
					APO10.01 Identificar y	Criterios para la identificación y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud			Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	evaluar las relaciones y contratos con proveedores.	categorización de proveedores.
					APO10.03 Gestionar contratos y relaciones con proveedores.	Criterios para el monitoreo de contratos y relaciones con terceros.
					APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01 Gestionar las Operaciones.	Establecer políticas y procedimientos para la entrega de servicios de TI.
					DSS05 Gestionar los Servicios de Seguridad.	Establecer políticas y procedimientos para la gestión de la seguridad de la información.
					DSS06 Gestionar los Controles de los Procesos de la Empresa.	Criterios para la definición y mantenimiento de controles a lo largo de los procesos de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	fundada y motivada de autoridad competente, informar de ese hecho al responsable.					
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario	Criterios para que los usuarios tengan los derechos apropiados

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					y el acceso lógico.	de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones		Art. 70	1. Recomendación General	DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.				DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la identidad del usuario y el acceso lógico.	Criterios para que los usuarios tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.
					MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Actividades para el monitoreo periódico del ambiente de control interno.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Actividades para el monitoreo del cumplimiento regulatorio, legal y contractual.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	APO09 Gestionar los Acuerdos de Servicio.	Criterios para el monitoreo y control de los acuerdos de servicio.
					APO10 Gestionar los Proveedores.	Criterios para la administración de proveedores de acuerdo a las necesidades de negocio.
					DSS01.01 Ejecutar procedimientos operativos.	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.
					DSS05.02 Gestionar la seguridad de la red y las conexiones.	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
					DSS05.03 Gestionar la seguridad de los puestos de usuario final.	Asegurar que los puestos de usuario final se encuentren asegurados para evitar mal uso de la información.
					DSS05.04 Gestionar la	Criterios para que los usuarios

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					identidad del usuario y el acceso lógico.	tengan los derechos apropiados de acceso a la información.
					DSS05.05 Gestionar el acceso físico a los activos de TI.	Criterios para que los usuarios tengan los derechos apropiados de acceso físico a la información.
					DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Criterios para el establecimiento de niveles de acceso y autorización dentro de los procesos de negocio.
					DSS06.06 Asegurar los activos de información.	Asegurar el acceso a los activos de información por métodos apropiados.

4.19 PCI DSS, Payment Card Industry Data Security Standard v2.0.

Introducción. Este estándar fue desarrollado por un comité conformado por las compañías de tarjetas bancarias más importantes, como una guía para las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, con el fin de asegurar dichos datos y prevenir fraudes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
					Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
					Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
					Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
					Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	3.2 No almacene datos confidenciales de autenticación después de recibir la autorización.	Guías para el borrado seguro de datos confidenciales del tarjetahabiente cuando ya no son necesarios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.					
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
FINALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	3.1 Almacene la menor cantidad posible de datos de titulares de tarjetas implementando políticas, procedimientos y procesos de retención y disposición de datos.	Guías para la definición de períodos de retención de datos y su borrado seguro.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
					Proteger los datos del	Guías para protección de datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					titular de la tarjeta.	del tarjetahabiente.
	El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
					Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
					Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
					Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.2 Establezca un proceso para identificar y asignar una clasificación de	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					riesgos para vulnerabilidades de seguridad descubiertas recientemente.	
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	12.1 Establezca, publique, mantenga y distribuya una política de seguridad.	Guías para la definición y comunicación de la política de seguridad.
					12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Guías para establecer las responsabilidades de seguridad de la información para el personal que procesa los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Guías para un programa forma de concienciación de seguridad de la información.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una revisión al menos una	Guías para la revisión de seguridad ante modificaciones

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					vez al año y actualizaciones al modificarse el entorno.	importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	12.3.1 Aprobación explícita por las partes autorizadas.	Guías para que se aprueben las políticas para el uso de tecnología.
					12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Revisión de que las políticas cuenten con responsabilidades para la seguridad de la información.
					12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los	Implementación del programa de concienciación de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					datos de titulares de tarjetas.	
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una	Guías para la revisión de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					revisión al menos una vez al año y actualizaciones al modificarse el entorno.	seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	12.3.1 Aprobación explícita por las partes autorizadas.	Guías para que se aprueben las políticas para el uso de tecnología.
					12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de	Revisión de que las políticas cuenten con responsabilidades para la seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de la información de todo el personal.	
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas.	Guías para la configuración de firewalls.
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas	Guías para el cifrado de datos durante su transmisión por redes abiertas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					abiertas.	
					Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
					Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
					Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten		Art. 48 - X	Paso 6. Identificación de las medidas de	10.2 Implemente pistas de auditoría automatizadas para	Guías para la verificación de pistas de auditoría en los sistemas y aplicaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	rastrear a los datos personales durante su tratamiento.			seguridad y Análisis de Brecha.	todos los componentes del sistema.	
					10.5 Resguarde las pistas de auditoría para evitar que se modifiquen.	Guías para el resguardo de las pistas de auditoría.
					10.6 Revise los registros de todos los componentes del sistema al menos una vez al día.	Guías para el monitoreo de los componentes de los sistemas.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	12.5 Asigne las siguientes responsabilidades de gestión de seguridad de la información a una persona o equipo.	Guías para la asignación de un responsable de la seguridad de la información en la organización.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá	Art. 19	Art. 4 Art. 9	Paso 6. Identificación de las	Requisito 1: Instale y mantenga una	Guías para la configuración de firewalls.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.		Art. 57	medidas de seguridad y Análisis de Brecha.	configuración de firewalls para proteger los datos de los titulares de las tarjetas.	
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
					Requisito 5: Utilice y actualice regularmente el software o los	Guías para la operación y mantenimiento de los esquemas de antivirus.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					programas antivirus.	
					Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras.	Guías para el desarrollo de aplicaciones seguras.
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					tarjetas.	
					Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	9.7.1 Clasifique los medios de manera que se pueda determinar la	Guías para la clasificación de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					confidencialidad de los datos.	
					9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.	Aprobación de los medios que contienen datos de los tarjetahabientes.
					9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Guías para el mantenimiento de inventarios de medios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	12.4 Asegúrese de que las políticas y los procedimientos de seguridad definan claramente las responsabilidades de seguridad de la información de todo el personal.	Guías para establecer las responsabilidades de seguridad de la información para el personal que procesa los datos del tarjetahabiente.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis	Requisito 1: Instale y mantenga una configuración de firewalls para	Guías para la configuración de firewalls.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				de Brecha.	proteger los datos de los titulares de las tarjetas.	
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
					Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
					Requisito 6:	Guías para el desarrollo de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Desarrolle y mantenga sistemas y aplicaciones seguras.	aplicaciones seguras.
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
					Requisito 11: Pruebe	Guías para revisar periódicamente

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					con regularidad los sistemas y procesos de seguridad.	la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una	Guías para llevar a cabo una evaluación formal de riesgos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					evaluación formal de riesgos.	
					12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					modificarse el entorno.	del tarjetahabiente.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos de los tarjetahabientes.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	12.6 Implemente un programa formal de concienciación sobre seguridad para que todos los empleados tomen conciencia de la importancia de la seguridad de los datos de titulares de tarjetas.	Guías para un programa forma de concienciación de seguridad de la información.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos	9.7.1 Clasifique los medios de manera que se pueda	Guías para la clasificación de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Personales.	determinar la confidencialidad de los datos.	
					9.8 Asegúrese de que la gerencia apruebe todos y cada uno de los medios que contengan datos de titulares de tarjetas que se muevan desde un área segura.	Aprobación de los medios que contienen datos de los tarjetahabientes.
					9.9.1 Lleve registros de inventario adecuadamente de todos los medios y realice inventarios de medios anualmente como mínimo.	Guías para el mantenimiento de inventarios de medios.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las	Guías para la configuración de firewalls.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					tarjetas.	
					Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.	Guías para no utilizar configuraciones por defecto de los proveedores.
					Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados.	Guías para la protección de datos durante su almacenamiento.
					Requisito 4: Cifrar transmisión de datos del titular de la tarjeta en las redes públicas abiertas.	Guías para el cifrado de datos durante su transmisión por redes abiertas.
					Requisito 5: Utilice y actualice regularmente el software o los programas antivirus.	Guías para la operación y mantenimiento de los esquemas de antivirus.
					Requisito 6: Desarrolle y mantenga sistemas y	Guías para el desarrollo de aplicaciones seguras.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					aplicaciones seguras.	
					Requisito 7: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	Guías para aplicar el mínimo privilegio para el acceso a los datos.
					Requisito 8: Asignar una ID exclusiva a cada persona que tenga acceso por computadora.	Guías para uso de identificadores únicos en la identificación y control de acceso.
					Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.	Guías para el acceso físico a los datos.
					Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.	Guías para el monitoreo y supervisión de los accesos a los datos y servicios de red.
					Requisito 11: Pruebe con regularidad los sistemas y procesos	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de seguridad.	de los tarjetahabientes.
					Requisito 12: Mantenga una política que aborde la seguridad de la información para todo el personal.	Guías para definir una política de seguridad con responsabilidades directas para el personal que maneja los datos de los tarjetahabientes.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías adicionales para el control de los proveedores de hosting compartido.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento.		Art. 62	Paso 8. Revisiones y Auditoría.	6.2 Establezca un proceso para identificar y asignar una clasificación de riesgos para vulnerabilidades de seguridad descubiertas recientemente.	Guías para la identificación y clasificación de riesgos antes vulnerabilidades de seguridad informática.
					Requisito 11: Pruebe con regularidad los sistemas y procesos	Guías para revisar periódicamente la seguridad de los sistemas y procesos que manejan los datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.				de seguridad.	de los tarjetahabientes.
					12.1.2 Incluya un proceso anual que identifique las amenazas, y vulnerabilidades, y los resultados en una evaluación formal de riesgos.	Guías para llevar a cabo una evaluación formal de riesgos.
					12.1.3 Incluye una revisión al menos una vez al año y actualizaciones al modificarse el entorno.	Guías para la revisión de seguridad ante modificaciones importantes de los sistemas y aplicaciones que manejan datos del tarjetahabiente.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	12.9.1 Cree el plan de respuesta a incidentes que será implementado en caso de que ocurra una violación de la seguridad del sistema.	Guías para un plan de respuesta a incidentes de seguridad.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad		Art. 50	1. Recomendación General.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable corresponderá al encargado.				Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas.	Guías específicas para la protección de los datos de los tarjetahabientes por parte de los proveedores de hosting compartido.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				tarjetas que ellos tienen en su poder.	
					12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	Guías para evaluar la capacidad del proveedor de servicios para proteger los datos del tarjetahabiente.
					Requisito A.1: Los proveedores de hosting compartidos deben proteger el entorno de datos de titulares de tarjetas.	Guías específicas para la protección de los datos de los tarjetahabientes por parte de los proveedores de hosting compartido.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	2.4 Los proveedores de servicio de hosting compartido deben proteger el entorno hospedado y los datos del titular de la tarjeta de la entidad.	Guías para evaluar que los proveedores de hosting compartido estén protegiendo los datos del tarjetahabiente.
					12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				12.8.3 Asegúrese de que exista un proceso establecido para comprometer a los proveedores de servicios que incluya una auditoría de compra adecuada previa al compromiso.	Guías para evaluar la capacidad del proveedor de servicios para proteger los datos del tarjetahabiente.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	Desarrollar y mantener una red segura.	Guías para tener una red segura de comunicaciones.
					Proteger los datos del titular de la tarjeta.	Guías para protección de datos del tarjetahabiente.
					Mantener un programa de administración de vulnerabilidad.	Guías para gestión de vulnerabilidades de seguridad.
					Implementar medidas sólidas de control de acceso.	Guías para el control de acceso.
					Supervisar y evaluar las redes con regularidad.	Guías para la revisión periódica de seguridad de la red.
					Mantener una política de seguridad de información.	Guías para definir y mantener una política de seguridad de la información.
					Requisitos de las PCI DSS adicionales para proveedores de hosting compartido (Anexo A).	Guías para controlar la seguridad cuando se emplean a proveedores de hosting compartido.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	12.8.2 Mantenga un acuerdo escrito que incluya una mención de que los proveedores de servicios son responsables de la seguridad de los datos de titulares de tarjetas que ellos tienen en su poder.	Guías para el establecimiento de acuerdos con los proveedores de servicios y para que sean responsables de la seguridad de los datos del tarjetahabiente.

4.20 HIPAA, Health Insurance Portability and Accountability Act.

Introducción. HIPAA es la Ley de Portabilidad y Responsabilidad del Seguro Médico, aplicable en Estados Unidos, su objetivo fundamental es facilitar a las personas mantener un seguro médico, proteger la confidencialidad y seguridad de la información médica, y ayudar a la industria de la salud a controlar los costos administrativos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
LICITUD Y LEALTAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	164.502 Usos y revelaciones de información protegida de salud: Reglas generales.	Disposiciones para usos y revelaciones solamente autorizados con respecto a la información de salud.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
					164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					individuo de acordar y objetar.	
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
					164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.				164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
					164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					y objetar.	
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	164.312(b) Controles de auditoría.	Mecanismos para registrar y examinar los sistemas que contienen información de salud.
					164.312(c)(1) Integridad.	Políticas y procedimientos para proteger la integridad información electrónica de salud.
					164.312(e)(1) Seguridad en la transmisión.	Medidas técnicas para la protección de la información de salud transmitida por la red.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
RESPONSABILIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					164.308(a)(1)(ii)(C) Política de sanción.	Aplicación de sanciones a quienes caen en incumplimiento con las políticas y procedimientos de seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	164.308(a)(5)(i) Entrenamiento y concientización de seguridad.	Implementación de un programa de entrenamiento y concientización de seguridad a todos los niveles de la organización.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
					164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	164.308(a)(1)(ii)(C) Política de sanción.	Aplicación de sanciones a quienes caen en incumplimiento con las políticas y procedimientos de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
					164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
					164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
					164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(a)(2) Asignación de la responsabilidad de seguridad.	Asignación de oficial de seguridad responsable del desarrollo e implementación de políticas y procedimientos de seguridad.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.					
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(D) Revisión de la actividad del sistema de información.	Procedimientos para la revisión de registros de sistemas de información que contienen información de salud.
					164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	164.310(d)(1) Controles en dispositivos y medios.	Políticas y procedimientos para la recepción y remoción de dispositivos y medios con información de salud.
					164.316(b)(1) Documentación.	Documentación de políticas y procedimientos para la protección de información de salud.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	164.308(a)(3)(ii)(A) Autorización y/o supervisión.	Procedimientos para la autorización y/o supervisión de empleados que acceden a información de salud.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
					164.316(b)(2)(iii) Actualizaciones.	Actualización periódica de la documentación ante cambios que afectan la seguridad de la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	164.308(a)(5)(i) Entrenamiento y concientización de seguridad.	Implementación de un programa de entrenamiento y concientización de seguridad a todos los niveles de la organización.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.310(d)(1) Controles en dispositivos y medios.	Políticas y procedimientos para la recepción y remoción de dispositivos y medios con información de salud.
					164.316(b)(1) Documentación.	Documentación de políticas y procedimientos para la protección de información de salud.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
					164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
					164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de salud.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
					164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría.	164.308(a)(6)(i) Procedimientos de	Políticas y procedimientos para el manejo de incidentes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.			Vulneraciones a la Seguridad de la Información.	incidentes de seguridad.	seguridad.
					164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
					164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
					164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.				164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
					164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
					164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad		Art. 50	1. Recomendación General.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
					164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
					164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
					164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Seguridad.	164.310 Salvaguardas físicas. 164.312 Salvaguardas técnicas.	Conjunto de controles físicos para la protección de información de salud. Conjunto de controles técnicos para la protección de información de salud.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para otorgar el acceso a las personas a su información de salud.
					164.308(b)(4) Contrato escrito.	Disposiciones para que las personas requieran la corrección de su información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.

4.21 SOx, Sarbanes-Oxley Act of 2002.

Introducción. La Ley SOx nace en Estados Unidos con para supervisar a las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversionista.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	Esta sección establece las responsabilidades corporativas de las empresas emisoras con respecto a los reportes financieros de resultados.
					Sección 404. Evaluación Gerencial de los Controles Internos.	Esta sección establece las obligaciones y responsabilidades de las empresas emisoras en la evaluación de sus controles internos con respecto a los reportes financieros de resultados.
LICITUD Y LEALTAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Medidas de Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas. (1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	por terceros con los que guarde alguna relación jurídica.					
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
					(a) Reglamentos requeridos.	
					(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
					(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	Sección 404. Evaluación Gerencial de los Controles Internos.	(b) Evaluación y reporte del Control Interno. Con respecto a la evaluación del control interno requerido, cada despacho contable que prepare o emita un reporte de auditoría para el emisor atestiguara, y reportará sobre la evaluación realizada por la Gerencia del emisor. Un atestiguamiento debe ser realizado de acuerdo con estándares para proyectos de atestiguamiento emitidos o adoptados por la PCAOB. Dicho atestiguamiento no será sujeto de un proyecto separado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
					(a) Reglamentos requeridos.	
					(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
					(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas.	(2) Contener una evaluación, a partir del más reciente año fiscal del emisor, de la efectividad de la estructura de control interno y los procedimientos del emisor para el reporte financiero.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que		Art. 48 - IX	Paso 6. Identificación de las medidas de	Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.			seguridad y Análisis de Brecha.	(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas. (1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Sección 404. Evaluación Gerencial de los Controles Internos. (a) Reglas requeridas. (1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá	Art. 19	Art. 4 Art. 9	Paso 6. Identificación de las	Sección 404. Evaluación Gerencial de los Controles Internos.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.		Art. 57	medidas de seguridad y Análisis de Brecha.	(a) Reglas requeridas.	
					(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
					(a) Reglamentos requeridos.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
					(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	NO APLICA	NO APLICA
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten	Sección 404. Evaluación Gerencial de los Controles Internos.	
					(a) Reglas requeridas.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Datos Personales.	(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
					(a) Reglamentos requeridos.	
					(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
					(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
36	Establecer las medidas de seguridad		Art. 61 - IV	Paso 6.	Sección 404. Evaluación Gerencial de los Controles Internos.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.			Identificación de las medidas de seguridad y Análisis de Brecha.	(a) Reglas requeridas.	
					(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Sección 404. Evaluación Gerencial de los Controles Internos.	
					(a) Reglas requeridas.	
					(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	Sección 404. Evaluación Gerencial de los Controles Internos.	
					(a) Reglas requeridas.	
					(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	Sección 404. Evaluación Gerencial de los Controles Internos.	
					(a) Reglas requeridas.	
					(2) Contener una evaluación, a partir del más reciente año fiscal del emisor, de la efectividad de la estructura de control interno y los procedimientos del emisor para el reporte financiero.	
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	NO APLICA	NO APLICA
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	Sección 404. Evaluación Gerencial de los Controles Internos.	
					(a) Reglas requeridas.	
					(1) Manifestar la responsabilidad de la Gerencia por el establecimiento y mantenimiento de una estructura adecuada de control interno y de procedimientos para el reporte financiero.	

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	Sección 302. Responsabilidad Corporativa por los Reportes Financieros.	
					(a) Reglamentos requeridos.	
					(5) Los funcionarios firmantes han divulgado a los auditores del emisor y al comité de auditoría de la junta de directivos (A) todas las deficiencias significativas en el diseño u operación de los controles internos las cuales podrían afectar negativamente la capacidad del emisor de registrar, procesar, resumir, y reportar datos financieros y han identificado para los auditores del emisor cualquier debilidad material en los controles internos.	
					(6) Los funcionarios firmantes han indicado en el reporte sí o no hubieron cambios significativos en los controles internos o en otros factores que pudieran significativamente afectar los controles internos posteriormente a la fecha de su evaluación, incluyendo cualquier acción correctiva con respecto a deficiencias significativas y debilidades materiales.	
VULNERACIONES A LA SEGURIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	NO APLICA	NO APLICA
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por		Art. 50	1. Recomendación General.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	datos personales sobre los que se preste el servicio.					
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio: c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Cotidiano de Medidas de Seguridad.		
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	NO APLICA	NO APLICA
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

4.22 ITIL, Information Technology Infrastructure Library v3.

Introducción. Es un conjunto de conceptos y prácticas en la gestión de servicios de tecnologías de la información, para lograr calidad y eficiencia en las operaciones. Su propósito fundamental es servir como guía para toda infraestructura, desarrollo y operación de Tecnología de la Información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
			RESPONSABLE			
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Estrategia del Servicio.	Procesos para la definición estratégica de los servicios de TI para la satisfacción de los clientes.
					Diseño del Servicio.	Procesos para el diseño de servicios de TI que satisfagan los requerimientos del negocio.
					Transición del Servicio.	Procesos requeridos para colocar un servicio de TI de manera operacional.
					Operación del Servicio.	Procesos requeridos para operar y mantener los servicios de TI conforme a lo acordado.
					Mejora continua del Servicio.	Procesos para medir y reportar el desempeño de los servicios de TI y mantener su valor para los clientes.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.					
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Cotidiano de Medidas de Seguridad		
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
					SD3.6.3 Diseño de la arquitectura tecnológica.	Prácticas para el diseño de la arquitectura tecnológica que cubra las necesidades presentes y futuras del negocio.
					SD3.9 Arquitectura orientada al servicio.	Prácticas para que los procesos y soluciones de negocio cuenten con un enfoque de arquitectura orientada al servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SD3.10 Gestión de servicio al negocio.	Prácticas para que los componentes de TI se encuentren ligados a los objetivos y metas del negocio.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					ST4.7 Gestión del conocimiento.	Prácticas recomendadas para la gestión del conocimiento necesario para la toma de decisiones.
					SD7 Consideraciones tecnológicas.	Recomendaciones para el uso de herramientas y técnicas en el diseño de servicios.
					SS6.5 Estrategia de sourcing.	Recomendaciones para definir la estrategia de outsourcing.
					SD3.5 Actividades de diseño.	Procesos principales para el diseño de servicios de TI.
					SD3.9 Arquitectura orientada al servicio.	
					SD3.11 Modelos para el diseño de los servicios.	Consideraciones para la adopción de un modelo para el diseño de los servicios.
					SD5.3 Gestión de aplicaciones.	Prácticas para la gestión efectiva de aplicaciones.
					ST3.2.3 Adopción de estándares y de un	Lineamientos para adoptar un estándar y un marco de trabajo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					marco de trabajo común.	común para la transición de servicios de TI.
					ST4.1.5.1 Estrategia de transición.	Recomendaciones para la adopción de una estrategia de transición de servicios de TI.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.6 Almacenamiento y archivo.	Prácticas para el almacenamiento y archivo de datos e información.
					SO5.2.3 Respaldo y restauración.	Prácticas para el respaldo y restauración de datos e información.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica,	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	sin que ello tenga como consecuencia la conclusión del tratamiento.					
PROPORCIONALIDAD						
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Estrategia del Servicio.	Procesos para la definición estratégica de los servicios de TI para la satisfacción de los clientes.
					Diseño del Servicio.	Procesos para el diseño de servicios de TI que satisfagan los requerimientos del negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.				Transición del Servicio.	Procesos requeridos para colocar un servicio de TI de manera operacional.
					Operación del Servicio.	Procesos requeridos para operar y mantener los servicios de TI conforme a lo acordado.
					Mejora continua del Servicio.	Procesos para medir y reportar el desempeño de los servicios de TI y mantener su valor para los clientes.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	SS7.5 Estrategia y mejora.	Aspectos de calidad al cliente a considerar en la definición de la estrategia del servicio de TI.
					SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
					SD4.6 Gestión de la	Prácticas recomendadas para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de la información.	gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					Apéndice E Detalles de la gestión de las instalaciones.	Lineamientos específicos para la gestión de instalaciones tanto de seguridad física como de control ambiental.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	SS6.4 Cultura organizacional.	Aspectos para incrementar la efectividad organizacional.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	SD6.3 Habilidades y atributos.	Recomendaciones para habilidades y atributos para los roles específicos de la gestión del servicio de TI.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						implementación.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
					CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
					CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
					SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
					SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD4.6.4 Políticas,	Conceptos básicos de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					principios y conceptos básicos.	seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
					CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
					CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SO4.1 Gestión de eventos.	Prácticas para la gestión de eventos en los servicios de TI.
					SO4.2 Gestión de incidentes.	Prácticas para la gestión de incidentes en los servicios de TI.
					SO6.2 Mesa de servicios.	Prácticas para la atención de eventos y solicitudes en los servicios de TI.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					ST3.2.13 Asegurar la calidad de un servicio nuevo o modificado.	Principios y mejores prácticas para lograr la calidad de un servicio nuevo o modificado.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.12 Gestión del	Aspectos a considerar para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					centro de datos e instalaciones.	gestión eficiente del centro de datos y las instalaciones.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	SO4.5 Gestión de acceso.	Prácticas y principios para la gestión de accesos para el uso de servicios.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD6.4 Roles y responsabilidades.	Roles y responsabilidades para el diseño de servicios de TI.
					SD4.6 Gestión de seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.				SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					Apéndice E Detalles de la gestión de las instalaciones.	Lineamientos específicos para la gestión de instalaciones tanto de seguridad física como de control ambiental.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y	Prácticas para el desarrollo de un Análisis de Impacto al

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				estrategia.	Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
					SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.4 Políticas, principios y conceptos básicos.	Conceptos básicos de seguridad de la información para ser implementados.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					ST4.3.5.3 Identificación de la configuración.	Aspectos a considerar para la identificación de los elementos de configuración de sistemas y aplicaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					SO5.2.4 Datos electrónicos e impresos.	Prácticas para el manejo de datos en formato electrónico e impreso.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	SO6.3 Gestión técnica.	Roles y responsabilidades para la gestión de la infraestructura de TI.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar		Art. 61 - IV	Paso 6. Identificación de las	SD3.6.1 Diseño de soluciones de	Actividades de diseño para un servicio nuevo o modificado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	aquéllas implementadas de manera efectiva.			medidas de seguridad y Análisis de Brecha.	servicios.	
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO4.5 Gestión de acceso.	Prácticas y principios para la gestión de accesos para el uso de servicios.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SO5.5 Gestión de redes.	Prácticas recomendadas para la gestión de las redes de comunicaciones.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	NO APLICA	NO APLICA
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
					CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
					CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
					SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
					SO5.13 Gestión de seguridad de la	Aspectos fundamentales de la seguridad de la información en

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información y la operación del servicio.	la operación del servicio.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	SD6.3 Habilidades y atributos.	Recomendaciones para habilidades y atributos para los roles específicos de la gestión del servicio de TI.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	ST4.3.5.3 Identificación de la configuración.	Aspectos a considerar para la identificación de los elementos de configuración de sistemas y aplicaciones.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	SD3.6.1 Diseño de soluciones de servicios.	Actividades de diseño para un servicio nuevo o modificado.
					SO4.4.5.11 Errores detectados en el entorno de desarrollo.	Manejo de los errores detectados en los entornos de desarrollo de sistemas y aplicaciones.
					SD4.6.5.1 Controles de seguridad.	Tipos de controles de seguridad recomendados para su implementación.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SD5.2 Gestión de los datos y la	Prácticas recomendadas para la gestión de la seguridad de la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					información.	información.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	CSI5.2 Evaluaciones.	Recomendaciones para evaluar los procesos operacionales contra los estándares de rendimiento de la organización.
					CSI5.3 Benchmarking.	Recomendaciones para evaluar los procesos operacionales contra las mejores prácticas del mercado.
					CSI5.4 Marcos de medición y reporte.	Prácticas para el uso de marcos de trabajo de medición y reporte de los procesos operacionales.
					SS9.5 Riesgos.	Identificación de tipos de riesgos a ser identificados y controlados.
					SD4.5.5.1 Etapa 1 – Inicio.	Aspectos para manejar los riesgos de continuidad de las operaciones de los servicios de TI.
					SD2.4.2 Alcance.	Aspectos para la definición del alcance del diseño del servicio.
					SD3.6 Aspectos de diseño.	Prácticas para el diseño de servicios con un enfoque integrado para cubrir su ciclo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de vida.
					SD4.5.5.2 Etapa 2 – Requisitos y estrategia.	Prácticas para el desarrollo de un Análisis de Impacto al Negocio y el tratamiento del riesgo de acuerdo a los objetivos del negocio.
					SO5.4 Gestión y soporte de servidores.	Prácticas recomendadas para la gestión y soporte de los servidores.
					SO5.5 Gestión de redes.	Prácticas recomendadas para la gestión de las redes de comunicaciones.
					SO5.7 Administración de bases de datos.	Prácticas recomendadas para la gestión de bases de datos.
					SO5.8 Gestión de servicios de directorio.	Prácticas recomendadas para la gestión de servicios de directorio.
					SO5.9 Soporte de estaciones de trabajo.	Actividades a considerar para el soporte de la operación de estaciones de trabajo.
					SO5.10 Gestión de middleware.	Prácticas recomendadas para la gestión de los componentes middleware de los servicios de TI.
					SO5.11 Gestión Internet/web.	Prácticas recomendadas para la gestión de servicios basados en web.
					SD4.6 Gestión de la	Prácticas recomendadas para la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					seguridad de la información	gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	SO4.5.5.6 Eliminar o restringir privilegios.	Aspectos a considerar en la eliminación o restricción de los privilegios de acceso.
					SO5.13 Gestión de seguridad de la información y la operación del servicio.	Aspectos fundamentales de la seguridad de la información en la operación del servicio.
					SD4.6.5.2 Gestión de brechas de seguridad e incidentes.	Consideraciones para la gestión de brechas e incidentes de seguridad de la información.
					SO4.4 Gestión de problemas.	Prácticas para la gestión de problemas presentados en la operación de los servicios de TI.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.		Art. 50	1. Recomendación General.	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
					SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
					SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
SUBCONTRATACIONES						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	del responsable corresponderá al encargado.					
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento;		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
					SD4.6 Gestión de la seguridad de la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de	SD4.2.5.9 Desarrollar contratos y relaciones.	Consideraciones para establecer contratos y desarrollar relaciones con terceros.
					SD4.7.5.3 Nuevos proveedores y contratos.	Aspectos para el manejo de nuevos proveedores y la formalización de contratos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Medidas de Seguridad.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
					SD4.6 Gestión de la seguridad de la información.	Prácticas para la gestión de proveedores.
					SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.12 Gestión del centro de datos e instalaciones.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD5.2 Gestión de los datos y la información.	Prácticas relacionadas con la gestión de los datos e información y el ciclo de vida del servicio.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.
					SO5.12 Gestión del centro de datos e instalaciones.	Aspectos a considerar para la gestión eficiente del centro de datos y las instalaciones.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SD4.2 Gestión de niveles de servicios.	Prácticas para la gestión de niveles de servicios.
					SD4.7 Gestión de proveedores.	Prácticas para la gestión de proveedores.
					SD5.2 Gestión de los datos y la información.	Prácticas recomendadas para la gestión de la seguridad de la información.

4.23 The Open Web Application Security Project (OWASP), Guía de Documentación v2.0.

Introducción. OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen al software inseguro. La Guía de Documentación provee lineamientos detallados sobre la seguridad de las aplicaciones web.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	NO APLICA	NO APLICA
CONSENTIMIENTO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba		Art. 20	Paso 7. Implementación de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	recaerá, en todos los casos, en el responsable.			las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.			Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.		
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	NO APLICA	NO APLICA
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
RESPONSABILIDAD						
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
					Pilares esenciales de la seguridad de la información.	Consideraciones de la integridad, disponibilidad, y confidencialidad de la información para la producción de un control robusto de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	relación jurídica.				Arquitectura de seguridad.	Integración de los pilares de integridad, disponibilidad, y confidencialidad de la información en el desarrollo de aplicaciones.
					Principios de seguridad.	Lineamientos fundamentales para el desarrollo seguro de aplicaciones.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de Seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	Educación del usuario.	Consideraciones para entrenar a los usuarios con respecto a la seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	NO APLICA	NO APLICA
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de Seguridad.
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio	Manejo de los pagos de una manera segura en sistemas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					electrónico.	comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Manejo de errores, auditoría, y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de	Guías para que la aplicación sea robusta frente a ataques de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					servicio.	negación de servicio.
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	Clasificación de activos.	Establece la selección de controles de seguridad con base en la clasificación de los datos a proteger.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	NO APLICA	NO APLICA
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	NO APLICA	NO APLICA
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	NO APLICA	NO APLICA
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	Clasificación de activos.	Establece la selección de controles de seguridad con base en la clasificación de los datos a proteger.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	NO APLICA	NO APLICA
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores.		Art. 62	Paso 8. Revisiones y Auditoría.	Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.					
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
					Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.				Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	Respuesta ante incidentes de seguridad.	Guías para el manejo de incidentes de seguridad.
					Arreglar problemas de seguridad correctamente.	Guías para eliminar vulnerabilidades de seguridad.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las		Art. 50	1. Recomendación General.	Arquitectura y diseño de seguridad.	Consideraciones para el establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado, y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	Compromiso organizacional con la seguridad.	Soporte de la alta gerencia para el desarrollo y adquisición de aplicaciones con principios básicos de seguridad.
51	Para el tratamiento de datos personales en		Art. 52 - II	Paso 7.	Arquitectura y diseño	Consideraciones para el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de			Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	de seguridad.	establecimiento de una arquitectura y diseño de seguridad para aplicaciones web.
					Principios de codificación segura.	Guías para la producción de aplicaciones seguras desde su diseño.
					Modelado de riesgo de amenaza.	Consideraciones para la incorporación de controles en las aplicaciones con base en amenazas y riesgos reales.
					Manejo de pagos en el comercio electrónico.	Manejo de los pagos de una manera segura en sistemas de comercio electrónico.
					Phishing.	Guías para la prevención del phishing.
					Servicios web.	Guías para el aseguramiento de servicios web.
					Autenticación.	Guías para proveer servicios de autenticación segura a las aplicaciones web.
					Autorización.	Guías para controlar el acceso a recursos protegidos mediante decisiones basadas en el rol o el nivel de privilegio.
					Manejo de sesiones.	Guías para que los usuarios autenticados cuenten con la protección de sus sesiones

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.					previniendo su reutilización, falsificación e intercepción de sesiones.
					Validación de datos.	Guías para que la aplicación sea robusta contra las formas de ingreso de datos.
					Intérprete de inyección.	Guías para que las aplicaciones sean seguras de ataques de manipulación de parámetros contra intérpretes comunes.
					Canonicalización, locales y Unicode.	Guías para que la aplicación sea robusta cuando esté sujeta a valores de entrada codificados, internacionalizados o en Unicode.
					Manejo de errores, auditoría y generación de logs.	Guías para que las aplicaciones sean auditables y permitan dar seguimiento a transacciones o accesos al sistema.
					Sistema de ficheros.	Guías para que el acceso local al sistema de ficheros esté protegido de creaciones, modificaciones o eliminaciones no autorizadas.
					Desbordamientos de memoria.	Guías para que las aplicaciones no se expongan a componentes defectuosos, cuenten con un manejo de memoria adecuado,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						y mecanismos para evitar el desbordamiento de memoria.
					Interfaces administrativas.	Guías para que las funciones de nivel de administrador estén segregadas de la actividad del usuario y para que los usuarios no puedan acceder o utilizar funcionalidades administrativas.
					Cifrado.	Guías para que el cifrado se use de manera segura para proteger la confidencialidad e integridad de los datos sensibles de usuarios.
					Configuración.	Guías para configurar las aplicaciones y su entorno de manera segura.
					Mantenimiento.	Guías para que las aplicaciones sean mantenidas correctamente después de su liberación y que los defectos de seguridad son arreglados correctamente y en un tiempo adecuado.
					Ataques de denegación de servicio.	Guías para que la aplicación sea robusta frente a ataques de negación de servicio.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	NO APLICA	NO APLICA
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA

4.24 Cloud Security Alliance Cloud Controls Matrix (CCM) v3.0.

Introducción. Esta matriz proporciona principios de seguridad para evaluar el riesgo de seguridad en un proveedor de cómputo en la nube. El marco de trabajo del documento ofrece controles divididos en 13 dominios.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Seguridad de la Aplicación y de Interfaz.	Conjunto de controles destinados a brindar seguridad a las aplicaciones y sus interfaces con otros sistemas.
					Aseguramiento de Auditoría y Cumplimiento.	Conjunto de controles para llevar a cabo la auditoría y revisión del cumplimiento de infraestructura de TI y de aplicaciones.
					Gestión de la Continuidad del Negocio y Capacidad de Recuperación Operacional.	Conjunto de controles para brindar continuidad del negocio y recuperación de los procesos que dependen de TI.
					Control de Cambios y Gestión de la Configuración.	Conjunto de controles para controlar cambios al ambiente operativo y gestionar la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						configuración de infraestructura de TI y aplicaciones.
					Seguridad de Datos y Gestión del Ciclo de Vida de la Información.	Conjunto de controles para brindar la seguridad de los datos y de la información durante su ciclo de vida.
					Seguridad del Centro de Datos.	Conjunto de controles físicos para la seguridad en los centros de datos.
					Gestión de Cifrado y Llaves.	Conjunto de controles para implementar cifrado de la información y gestión de las llaves de cifrado.
					Gobierno y Gestión de Riesgo.	Controles y actividades para gestión de riesgos de seguridad, y de cumplimiento regulatorio.
					Recursos Humanos.	Controles y prácticas para contar con seguridad en las relaciones con los empleados.
					Gestión de Identidades y Accesos.	Controles para la gestión de identidades de los usuarios y procesos, y el control de acceso a la infraestructura de TI y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						aplicaciones.
					Infraestructura y Seguridad en la Virtualización.	Controles para dar seguridad en ambientes virtualizados.
					Interoperabilidad y Portabilidad.	Controles y prácticas para brindar interoperabilidad y portabilidad a las aplicaciones que funcionan en un esquema de cómputo en la nube.
					Seguridad Móvil.	Controles y prácticas para la seguridad por el uso de dispositivos móviles.
					Gestión de Incidentes de Seguridad, Forense en la Nube, y Descubrimiento Electrónico.	Controles y prácticas para la detección y atención de incidentes de seguridad.
					Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.	Gestión de terceros que participan como proveedores para brindar los servicios de cómputo en la nube a los clientes finales.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Gestión de Amenazas y Vulnerabilidades.	Controles y prácticas para el manejo adecuado de amenazas y vulnerabilidades de seguridad informática.
LICITUD Y LEALTAD						
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.				AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.					
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	NO APLICA	NO APLICA
9	El aviso de privacidad debe contener un	Art. 18	Art. 14	Paso 7.	AIS-04 Seguridad de	Políticas y procedimientos para

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.		Art. 29 Art. 32	Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	Datos / Integridad.	brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					CCC-03 Prueba de Calidad.	Actividades de monitoreo y evaluación del cumplimiento de estándares de calidad y de líneas base de seguridad.
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	presente el mencionado incumplimiento.				DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad	BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos e información.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
RESPONSABILIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	NO APLICA	NO APLICA
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
					HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
					HRS-10	Definición de un programa

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Entrenamiento / Concientización.	formal de entrenamiento y concientización en seguridad de la información.
					SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	NO APLICA	NO APLICA
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	AIS-01 Seguridad de la aplicación.	Consideraciones para el desarrollo seguro de aplicaciones.
					AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-03 Integridad de datos.	Integración de rutinas en las aplicaciones para prevenir errores de procesamiento de datos.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-04 Documentación.	Documentación necesaria para la instalación, configuración, y operación de sistemas de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información.
					CCC-01 Nuevos desarrollos / Adquisición.	Políticas y procedimientos para aceptar la adquisición de soluciones o nuevos desarrollos.
					CCC-05 Cambios en producción.	Establecimiento de un procedimiento de control de cambios para no introducir errores y problemas de seguridad en los ambientes productivos.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-06 Datos no operacionales.	Políticas y procedimientos para impedir el uso de datos en ambientes no operacionales.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-04 Seguridad de	Políticas y procedimientos para

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					Datos / Integridad.	brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	SEF-01 Contacto / Mantenimiento con la autoridad.	Establecimiento de contactos, incluyendo autoridades, para el manejo de incidentes de seguridad.
					SEF-02 Gestión de incidentes.	Políticas y procedimientos para la detección y manejo de incidentes de seguridad.
					SEF-03 Reporte de incidentes.	Establecimiento de medios de comunicación para el reporte de incidentes de seguridad.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto		Art. 48 - IX	Paso 6. Identificación de las	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad,

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.			medidas de seguridad y Análisis de Brecha.		integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
					BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						autorizada de SW en equipos de cómputo.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de	Procedimientos para evitar el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					personal no autorizado.	ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-07 Mantenimiento de	Políticas y procedimientos para el mantenimiento adecuado de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					equipo.	equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	NO APLICA	NO APLICA

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad.		
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las disposiciones relativas a las medidas de	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
					BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	seguridad contenidas en el Capítulo III de Reglamento.					del servicio y las operaciones de TI.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	Políticas, procedimientos, y medidas técnicas para la protección de datos sensibles durante su uso, transmisión, y almacenamiento.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.				STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y	HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Obligaciones de Quienes Traten Datos Personales.		empleados.
					HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad de la información en contratos laborales.
					HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
					SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones	Protección de los datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					de Comercio Electrónico.	utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
				Seguridad Faltantes.	DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					SEF-01 Contacto / Mantenimiento con la autoridad.	Establecimiento de contactos, incluyendo autoridades, para el manejo de incidentes de seguridad.
					SEF-02 Gestión de	Políticas y procedimientos para

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					incidentes.	la detección y manejo de incidentes de seguridad.
					SEF-03 Reporte de incidentes.	Establecimiento de medios de comunicación para el reporte de incidentes de seguridad.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
					TVM-01 Antivirus / SW malicioso.	Políticas y procedimientos para combatir virus y SW malicioso.
					TVM-02 Vulnerabilidades / Gestión de parches.	Políticas y procedimientos para la gestión de parches de seguridad y eliminación de vulnerabilidades.
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	HRS-02 Revisión de antecedentes.	Lineamientos para la revisión de antecedentes de los empleados.
					HRS-03 Acuerdos de empleo.	Inclusión de responsabilidades de seguridad y confidencialidad

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de la información en contratos laborales.
					HRS-10 Entrenamiento / Concientización.	Definición de un programa formal de entrenamiento y concientización en seguridad de la información.
					SEF-05 Métricas para Respuesta a Incidentes.	Mecanismos para cuantificar los tipos, cantidad, y costos de los incidentes de seguridad.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					BCR-05 Riesgos Ambientales.	Protección física contra causas y desastres naturales.
					BCR-07 Mantenimiento de	Políticas y procedimientos para el mantenimiento adecuado de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					equipo.	equipos para lograr la continuidad y disponibilidad de las operaciones.
					BCR-11 Política.	Definición de políticas y procedimientos para la gestión del servicio y las operaciones de TI.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					CCC-04 Instalación de SW no autorizado.	Políticas y procedimientos para restringir la instalación no autorizada de SW en equipos de cómputo.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DCS-02 Puntos controlados de acceso.	Implementación de perímetros físicos de seguridad para el control de acceso.
					DCS-06 Política.	Políticas y procedimientos para un ambiente seguro en oficinas e instalaciones.
					DCS-07 Autorización a áreas seguras.	Monitoreo y control de acceso a las áreas restringidas.
					DCS-08 Ingreso de personal no autorizado.	Procedimientos para evitar el ingreso no autorizado de personal a áreas seguras.
					DCS-09 Acceso de usuarios.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					EKM-03 Protección de datos sensibles.	El acceso físico de los usuarios a los servidores productivos debe ser evitado.
					IAM-05 Segregación de funciones.	Políticas y procedimientos para evitar conflictos de segregación de funciones en la ejecución de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						tareas.
					IAM-09 Autorización de acceso de usuarios.	Proceso formalizado para otorgar el acceso autorizado a los datos e información.
					IAM-10 Revisión de accesos de usuarios.	Revisión periódica de los accesos y privilegios de los usuarios a los datos e información.
					IAM-11 Revocación de accesos de usuarios.	Proceso formalizado para revocar en tiempo y forma el acceso a los datos e información.
					IVS-01 Registros de auditoría / Detección de intrusos.	Procedimientos para el registro de eventos de seguridad y su análisis para la detección de intrusos.
					IVS-06 Seguridad de la red.	Medidas para proteger las redes de ataques de seguridad informáticos.
					IVS-12 Seguridad inalámbrica.	Políticas y procedimientos para proteger las redes inalámbricas de ataques de seguridad informáticos.
43	Actualizar las medidas de seguridad cuando:		Art. 62	Paso 8. Revisiones y	AIS-01 Seguridad de	Consideraciones para el

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.			Auditoría.	la aplicación.	desarrollo seguro de aplicaciones.
					AIS-02 Requerimientos para el acceso de clientes.	Revisión de que todos los requerimientos técnicos, legales, etc. se satisfacen antes de otorgar acceso al cliente a los datos e información.
					AIS-03 Integridad de datos.	Integración de rutinas en las aplicaciones para prevenir errores de procesamiento de datos.
					AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-03 Mapeo regulatorio de sistemas de información.	Inventario de obligaciones legales y regulatorias de la organización asociadas con la infraestructura de TI y aplicaciones.
					BCR-04 Documentación.	Documentación necesaria para la instalación, configuración, y operación de sistemas de información.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					CCC-01 Nuevos desarrollos / Adquisición.	Políticas y procedimientos para aceptar la adquisición de soluciones o nuevos desarrollos.
					CCC-05 Cambios en producción.	Establecimiento de un procedimiento de control de cambios para no introducir errores y problemas de seguridad en los ambientes productivos.
					DSI-01 Clasificación.	Clasificación de los datos de acuerdo a su sensibilidad.
					DSI-06 Datos no operacionales.	Políticas y procedimientos para impedir el uso de datos en ambientes no operacionales.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					GRM-10 Evaluaciones de riesgo.	Lineamientos para llevar a cabo las evaluaciones del riesgo de seguridad de la información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata.		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	V. Los medios donde puede obtener más información al respecto.					
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
ENCARGADO						
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:		Art. 50	1. Recomendación General.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.					los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-07 Mantenimiento de equipo.	Políticas y procedimientos para el mantenimiento adecuado de equipos para lograr la continuidad y disponibilidad de las operaciones.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					DSI-08 Disposición Segura.	Políticas y procedimientos para la eliminación segura de datos

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						e información.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
SUBCONTRATACIONES						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.			Seguridad.	DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
CÓMPUTO EN LA NUBE						
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					DSI-03 Transacciones de Comercio Electrónico	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política	Políticas y procedimientos para el etiquetado y manejo de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				de Seguridad.	datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						confidencialidad los datos e información.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					AAC-02 Auditorías Independientes.	Revisiones y evaluaciones independientes para solucionar las no conformidades de la organización en su normatividad interna y externa.
					BCR-12 Política de Retención.	Políticas y procedimientos para la retención de datos e información de acuerdo con la normatividad aplicable.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política	Políticas y procedimientos para el etiquetado y manejo de los

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.				de Seguridad.	datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					GRM-09 Revisión de políticas.	Lineamientos para la revisión y actualización de políticas de seguridad de la información.
					HRS-07 Acuerdos de confidencialidad.	Establecimiento de acuerdos de confidencialidad para la protección de los datos e información.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-05 Acuerdos de la cadena de suministro.	Formalización de acuerdos de niveles de servicio entre los participantes que proveen los servicios de cómputo en la nube.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
TRANSFERENCIAS						
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones		Art. 70	1. Recomendación General	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.
					DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.				DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad	AIS-04 Seguridad de Datos / Integridad.	Políticas y procedimientos para brindar confidencialidad, integridad y disponibilidad de los datos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	condiciones en las que el titular consintió el tratamiento de sus datos personales.			Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	DSI-03 Transacciones de Comercio Electrónico.	Protección de los datos utilizados en el comercio electrónico contra su uso no autorizado.
					DSI-04 Manejo / Etiquetado / Política de Seguridad.	Políticas y procedimientos para el etiquetado y manejo de los datos e información de acuerdo con su criticidad.
					DSI-05 Fuga de información.	Implementación de mecanismos para prevenir la fuga de información y datos.
					IAM-07 Acceso a terceros.	Políticas y procedimientos para el otorgamiento del acceso a terceros a los datos e información.
					STA-09 Auditorías de terceros.	Auditorías de revisión a terceros o proveedores que se utilizan para la prestación de servicios de cómputo en la nube, y determinar si manejan con seguridad y confidencialidad los datos e información.

5. ANEXO - Definiciones

Las definiciones aquí enunciadas derivan de conceptos relevantes previstos en la Ley Federal de Protección de Datos en Posesión de los Particulares y su Reglamento, así como de otros que se consideraron importantes incorporar al presente documento:

Aviso de Privacidad: El documento físico, electrónico o en cualquier otro formato generado por el Responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con la obligación establecida en la Ley.

Bases de Datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Confidencialidad: La protección de los datos personales para evitar su divulgación no autorizada. Esto significa que los datos personales no podrán ser conocidos por quien no esté explícitamente autorizado para ello por el titular o por alguna disposición legal.

Consentimiento: La manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Datos Personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos Personales Sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquéllos que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición que los titulares tienen respecto de sus datos personales que trata el responsable.

Disponibilidad: Se refiere a que la información sea accesible cuando sea requerida.

Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Instituto: El Instituto Federal de Acceso a la Información y Protección de Datos, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Integridad: La protección de la información de alteraciones no autorizadas.

Ley o LFPDPPP: La Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Protección de Datos Personales: La totalidad de medidas encaminadas a asegurar los derechos de los titulares en el tratamiento de sus datos personales.

Reglamento: El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Responsable: La persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Tercero: La persona física o moral, nacional o extranjera, distinta del titular, del responsable o del encargado.

Titular: La persona física a quien corresponden los datos personales.

Transferencia: Toda comunicación de datos personales realizada a persona distinta del titular, responsable o encargado del tratamiento.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. En el entendido que el uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de Datos Personales.